Refine Search

Search Results -

Terms	Documents
L13 and 235/379	60

Database:
US Pre-Grant Publication Full-Text Database
US Patents Full-Text Database
US OCR Full-Text Database
EPO Abstracts Database
JPO Abstracts Database
Derwent World Patents Index
IBM Technical Disclosure Bulletins

Search:

Refine Search

Recall Text Clear Interrupt

Search History

DATE: Friday, June 23, 2006 Printable Copy Create Case

Set Name side by side	Query	Hit Count	Set Name result set
DB=PGPB,USPT,USOC,EPAB,JPAB,DWPI,TDBD; PLUR=YES; OP=OR			
L28	l13 and 235/379	60	L28
L27	235/379	5601	L27
L26	l13 and 705/43	17	L26
L25	l14 and 705/43	16	L25
L24	L15 and 235.clas.	21	L24
L23	L15 and 345.clas.	0	L23
L22	L15 and 345/700	0	L22
L21	L15 and 235/380	15	L21
L20	L15 and 235/375	5	L20
L19	L15 and 705/1	23	L19
L18	L15 and 705/44	6	L18
L17	L15 and 705/42	2	L17
L16	L15 and 705/43	5	L16

L15	L14 and authorization with request	127	L15
L14	L13 and transaction	792	L14
L13	L12 and ("pda" or "personal digital assistant" or personal with digital with assistant or personal adj digital adj assistant)	1315	L13
L12	L11 and (communication with port or communication near port or communication adj port)	8122	L12
L11	("atm" or "automated teller machine" or self-service with terminal or "self-service terminal")	150337	L11
L10	345/700	1235	L10
L9	345.clas.	75920	L9
L8	235/380	9056	L8
L7	235/375	7353	L7
L6	235.clas.	95610	L6
L5	705.clas.	42672	L5
L4	705/1	5896	L4
L3	705/44	1124	L3
L2	705/42	667	L2
L1	705/43	615	L1

END OF SEARCH HISTORY

L14: Entry 701 of 792 File: USPT Aug 5, 2003

DOCUMENT-IDENTIFIER: US 6604087 B1
TITLE: Vending access to the internet, business application software, e-commerce, and e-business in a hotel room

Abstract Text (1):
The present invention relates to a universal advertising and payment system and method for networking, monitoring and effectuating electronic commerce and controlling vending equipment. The system can effectuate electronic commerce and interactive advertising at the point of sale. Vending equipment can include vending access to the Internet, business application software, e-commerce, and e-business in a hotel room. In addition, vending equipment includes copiers, phones, facsimile machines, printers, data-ports, laptop print stations, notebook computers, palmtop computers (PALM PILOT), microfiche devices, projectors, scanners, cameras, modems, communication access, cellular phones, personal data assistants (PDA's), pagers, vending machines, personal computers (PC), PC terminals (NET PC), and network computers (NC). Vending equipment can be networked to each other through a first network, programmable and accessible by a PC, server, point of sale (POS) system, property or management information system (PMS/MIS), and networked to a second network. The first network and second network can be the same network. Complete control of a vending machine's functionality including usage, control, diagnostics, inventory, and marketing data capture can be effectuated locally or by remote connection to the network. Remote connection to the network includes Internet type connections, telecommunication (telephone, ISDN, ADSL), VSAT satellite, and other wire and wireless transmission.

Brief Summary Text (9):
An "unmanned" business center can be open for business 24-hours a day. This type of center typically relies on coin-cash-card systems to activate the business center's equipment. The type of card accepted is a magnetic card which includes a credit card, a smart card, a debit card, a pre-paid, automated teller machine ("ATM") or other bank or private issued card. Coin-cash-card systems are well known for copiers, however, for faxing, PC's, and other types of vending equipment and services, reliance on these types of systems alone can be awkward and in certain situations impractical. As a result, certain services such as faxing, and computing may not be available to customers, or offered to customers with limited service functionality.

Brief Summary Text (10):
An "unmanned center" relying on coin activated copiers and fax machines may offer little in the way of security and safety to the equipment. Furthermore, by accumulating money in coin boxes, the risk of break-ins, damage and theft can be increased. A service attendant may be required to remove money from the coin boxes at a periodic interval, adding an additional level of labor, and increasing the potential of theft. Also, customers using a coin or cash operated business center could find themselves without sufficient monetary means to pay for products and services, as coin changers and ATMs, or other cash access means may not be readily available.

Brief Summary Text (17):
The present invention is embodied in a simple and effective system and method for a

universal control and payment system to distribute and display interactive advertising, conduct electronic commerce, and control the billing for the use of vending equipment. Vending equipment can include vending access to the Internet, business application software, e-commerce, and e-business in a hotel room. In addition, vending equipment can include copiers, phones (public, private, cellular), facsimile machines, printers, data-ports, laptop print stations, notebook computers, palmtop computers (PALM PILOT), microfiche devices, projectors, scanners, cameras, modems, communication access, personal data assistants (PDA's), pagers, and other types of vending machines, personal computers (PC), PC terminals (NET PC), and network computers (NC).

Brief Summary Text (18):
One aspect of the present invention provides a system for public access to electronic commerce. More specifically, the present invention can control, monitor, and effectuate electronic commerce transactions such that the general public can use the present invention as a public access electronic commerce station.

Brief Summary Text (19):
Another aspect of the present invention provides the ability to route credit card and other types of transactions, allowing credit card and other types of transactions to be processed in an offline, or online environment.

Drawing Description Text (12):
FIGS. 9A-9B shows a customer transaction routine 700 flowchart;

Drawing Description Text (14):
FIG. 11 shows a transaction routing routine 900 flowchart;

Drawing Description Text (20):
FIG. 17 shows a POST-VEND transaction processing routine 1500 flowchart; and

Detailed Description Text (3):
A vending machine is defined as any piece of equipment in which products and/or services can be rendered therefrom. Referring again to FIG. 1, control of a vending machine (referred to as VENDING MACHINE USAGE) can involve a first step of denying usage, access, service, or products from the vending machine as shown in step 10. Next, in step 20 the system accepts user input (data and/or monetary, disclosed herein as PRE-VEND TRANSACTION DATA (i.e. "AUTHORIZATION")), and then in step 30, the system authenticates or verifies the user's input to determine if VENDING MACHINE USAGE is "authorized." If, in step 40, VENDING MACHINE USAGE is "authorized" the processing proceeds to step 50. In step 50, the system effectuates the delivery, monitoring, and dispensing of the product, and/or service. Then, in step 60, the system processes the POST-VEND TRANSACTION DATA to effectuate user (customer) billing, and account maintenance. Lastly, in step 70, the system "settles" (effectuates the transfer of funds, i.e. payment) the POST-VEND TRANSACTION DATA.

Detailed Description Text (4):
Step 70 can be optional when a PRE-VEND TRANSACTION can both satisfy the requirements of step 40, "authorization" and step 70, "settling." Examples of when Step 70 may not be required, can include vending of a product or service when at the time of creating the PRE-VEND TRANSACTION DATA (i.e. the "authorization") the exact amount of the total sale is known. Other examples of when step 70 may not be required can include creating PRE-VEND TRANSACTION DATA (i.e. the "authorization") where no bill for the product or service will be incurred by the user (customer) (i.e. products and/or services for a particular user are "free").

Detailed Description Text (5):
One example of a vending machine is shown in FIG. 2, a personal computer system, known as a system 100. The arrangement on table 129 is comprised of a PC 102, a

monitor 128, a transaction control device 108 (shown in an exemplary embodiment as a combination of a magnetic card terminal 136 and debit card reader-writer 134 packaged together), a keyboard 110, a modem 114, a mouse 112, a printer 104 and a controller 106.

Detailed Description Text (6):
A reliable way to govern the use of a PC system and its various components is to effectuate control of the mouse 112, keyboard 110, printer 104, modem 114, telecommunication lines (phone, ISDN, asymmetric digital subscriber line) and other peripheral devices. A PC system which has a mouse and keyboard under regulated control of a transaction control device 108 (such transaction control device capable of placing the mouse and keyboard in an inoperable state) can effectively prevent unauthorized use of the PC system. With an inoperable keyboard, an unauthorized user can not make typographic input. Furthermore, an inoperable mouse prevents an unauthorized user from selecting functions or features, entering selections or choices or executing control of software programs. To further enhance and secure a PC system, regulating control of other components of the PC system can also be implemented.

Detailed Description Text (7):
A transaction control device 108 is defined as any device that can accept coins, currency, magnetic cards, smart cards, credit cards, debit cards or other value storing medium and is capable of communicating a set of qualifying/disqualifying data or enabling/disabling data to a second control device. Transaction control devices such as a debit card reader-writer, a coin or currency activated device or a credit card terminal provide a means for indicating to external peripheral devices that a set of satisfying criteria has been met and allowance of system use is granted (an enabling signal).

Detailed Description Text (11):
Vended products from a vending machine can include usage time, device usage count, printed output, copies, printed pages, fax transmissions, and other related supplies (e.g. food, beverage, staplers, film, rubber bands, paper clips, note pads, computer disks, pens, and pencils). Vended services from a vending machine can include charging for usage time of a PC-NET PC-NC 630, charging for usage time of online services, access to program applications, or databases, and charging for electronic commerce transactions.

Detailed Description Text (12):
A public access electronic commerce terminal is a computing device, such as a system 500. FIGS. 3 and 3A show exemplary embodiments of electronic commerce terminal system 500. A public access electronic commerce terminal can be referred to as an electronic commerce terminal. A public access electronic commerce terminal can effectuate control of a vending machine as required while allowing a user of the system to view, vend, respond to, or purchase from displayed interactive advertising. Furthermore, a user can make general inquires and obtain other information related to the interactive advertising from a public access electronic commerce terminal. A system 500 can be a public access electronic terminal. A system 500 can also be a transaction control device, such as a transaction control device 108. An E-PORT manufactured by USA TECHNOLOGIES can be a system 500.

Detailed Description Text (13):
The ability to view, vend, obtain information, respond to, or purchase from displayed interactive or electronic advertising by way of an electronic computing device is generally referred to as an electronic commerce transaction or as electronic commerce. A system 500 can also be an electronic computing device.

Detailed Description Text (14):
A typical business center can be comprised of a plurality of vending equipment. A business center can include a copier 602A, a fax machine 604A, a laptop/palmtop

print station 646, a data-port/phone 648, and a PC-NET PC-NC 630 (PC 630). Furthermore, many business centers and retail outlets (store or location) require a plurality of copiers 602, a plurality of faxes 604, a plurality of PCs 630, and other vending equipment to meet the needs of their customers. A control system, and operational method which can interface and control a plurality of different types of vending equipment is also required. It is also desirable that each vending machine is networked to share resources and reduce undue duplication, and expense of equipment. For example, when printing a customer receipt is required, a single printer on the network can allow a plurality of vending machines to share the single printer. Furthermore, networking vending machines in a business center, or a retail outlet facility enables shared transaction processing capabilities and allows system integration with existing POS, PMS/MIS, and other network systems. A management information system (MIS) can be a POS system or a PMS system.

Detailed Description Text (23):
In an exemplary embodiment, a service technician with a hand held device could record system readings and program functionality of any system 500 controller and/or a network server. By using a hand-held device to data communicate with infrared communications means 502, a technician can upload or download data including program code, service data, transaction data, and other operational data.

Detailed Description Text (31):
Interconnected with microcontroller 532 is an electrically erasable read only memory ("EEROM") 516. Such an EEROM 516 can be a MICROCHIP 93LC66 serial EEROM. Interconnected with microcontroller 532 is a non-volatile memory 518. Such a non-volatile memory 518 can be a DALLAS SEMICONDUCTOR DS1643-120 or DS-1743. Furthermore, the DS1643-120 or DS-1743can provide a non-volatile date and time function whereby microcontroller 532 can be responsive to events based on date and time and date and time stamp transactions as they occur.

Detailed Description Text (37):
Interconnected with microcontroller 532 is an auxiliary terminal interface control means 530 for interfacing with a transaction control device 108.

Detailed Description Text (38):
Interconnected with microcontroller 532 is a plurality of input devices including a voice and/or handwriting capture and recognition means 534, a bar code reader 536, a fingerprint/palm/hand reader biometric means 538, and a keypad 540. Each of these input devices performs the indicated function independent of microcontroller 532 and by way of data communications with microcontroller 532 data communicates results of the input function to microcontroller 532 for interpretative post processing. Handwriting capture and analysis processing allows a system 500 to capture a customer's signature. Operating on the captured signature an analysis or customer validating process can be performed. Furthermore, the captured signatures can be utilized for authorization of the transaction and for credit card processing purposes.

Detailed Description Text (44):
Interconnected with microcontroller 532 is a plurality of card and key readers and writers including smart card reader/writer 548, magnetic card reader/writer 550, debit card reader/writer 552 and a hotel room key/card interface 554. Each interface accepts a form of customer identification and data communicates with microcontroller 532. A smart card reader/writer 548 can be a GEMPLUS GCR400, or a GEMPLUS GCI400, or a NEURON MSR-100, or a NEURON MSR-270 series. A magnetic card reader/writer 550 can be a XICO 7102ESA, or a XICO 6272SA, or a NEURON MSR-100, or a NEURON MSR-270 series, or a NEURON MCX-370-1R-0101. A debit card reader/writer 552 can be a DEBITEK, DAYNL, SCHLUMBERGE, ACT, XCP, ITC, COPICARD brand of debit card reader/writer, or other transaction control device 108.

Detailed Description Text (45):
Interconnected with microcontroller 532 is a local area network (LAN) network control means 556. A LAN network connection means 556 includes a wireless communication means 558, a carrier current communication means 560 and a hardwired communication means 562. A wireless transceiver means 558 can be a WIRELESS TRANSACTION CORPORATION WCC-1200, WTC-1300, STU-200, or a STU-300. A carrier current communication means 560 can be effectuated with traditional carrier current technologies, or spread spectrum technologies. Such a communication means 560 can be implemented as desired and known to one skilled in the art. A hardwired transceiver control means 562 can be implemented by way of the RS232 standard serial communication, or RS485 serial communication. RS485 data communication can be effectuated with a pair of wires (DATA "A" wire and DATA "B" wire). Further, a hardwired communication means 562 can be implemented using Ethernet, token ring, TCP/IP, Net Buoy or other networking scheme as is known to one skilled in the art.

Detailed Description Text (47):
Interconnected are a first communication means 564 and a second communication means 566. The first and second communication means 564 and 566 can be PARALLEL, RS232, RS485, PCMCIA, LAN or other standard communication ports. Interconnection to peripheral devices can include printers, network controllers, hand-held devices, and PC's 630. A first and second communication means 564 and 566 can be implemented with a SIPEX SP235A (RS232-TTL converter) or a MAXIM MAX244CQH, and/or a MAXIM MAX481 (RS485 converter)

Detailed Description Text (52):
Interconnected with microcontroller 532 is a first display 582. First display 582 can be a liquid crystal display (LCD), wherein transaction information and advertising can be displayed. A first display 582 can be implemented by way of an OPTREX #DMF-5002NY-EB super-twist graphics module, or an OPTREX #DMC-6204NY-LY liquid crystal display, or a OPTREX #DMF-50944NCU-FW-1 and an EPSON SED1354FOA LCD controller.

Detailed Description Text (65):
Interconnected with a printer 612A is the first local area network (LAN) 622. The printer 612A can be a system 500 in combination with a printer, or print mechanism. In an exemplary embodiment, a printer 612A can be a general-purpose printer for use by a customer, and/or any system 500 device on network 600. Any vending machine or universal server on the first LAN 622 or the second local area network (LAN) 626 can also access and data communicate with the printer 612A. Applications for the printer 612A can include general-purpose printing, transaction receipt printing, hotel/retail outlet summary report printing, advertisement printing, coupon printing, computer/notebook/laptop/palmtop printing, and hotel/retail outlet activity report printing.

Detailed Description Text (66):
Interconnected with a printer 612B is the second LAN 626. The printer 612B can be a system 500 in combination with a printer. In an exemplary embodiment, a printer 612B can be a general-purpose printer for use by a customer, and/or any system 500 on network 600. Furthermore, any vending machine or universal server on the first LAN 622, or the second LAN 626 can utilize printer 612B. Applications for the printer 612B can include general purpose printing, transaction receipt printing, hotel/retail outlet summary report printing, advertisement printing, coupon printing, computer/notebook/laptop/palmtop printing, and hotel/retail outlet activity report printing.

Detailed Description Text (70):
Interconnected with an information/Internet kiosk 628 is the second LAN 626. The information/Internet kiosk 628 can include a system 500 in combination with a PC 630 or other computer data communication equipment. In an exemplary embodiment, the information/Internet kiosk and a system 500 interconnected in combination with the

information/Internet kiosk 628 can effectuate electronic commerce transactions (payment, shipping, ordering, etc.). Additionally, such a system can provide access to and can effectuate transactions for products and services including other on-line, and/or off-line transactions (i.e. travel information, coupons, advertising, general use, entertainment, business, etc.).

Detailed Description Text (71):
Interconnected with a PMS/MIS system 620 can be a system 500D. A system 500D can be a system 500. A further interconnection exists between the system 500D and the first LAN 622. In an exemplary embodiment, the PMS/MIS system 620 can allow centralized programming and control of the network 600. The PMS/MIS system 620 can manage data processing needs of the network 600, can store and allow modification of vending machine settings, and implement gathering and maintain marketing, customer survey and other informational databases. Furthermore, PMS/MIS system 620 can support transaction processing, and/or implement the universal server functionality.

Detailed Description Text (73):
Interconnected with a point of sale (POS) system 614 can be a system 500I. A system 500I can be a system 500. A further interconnection exists between the system 500I and the first LAN 622. In an exemplary embodiment, the POS system 614 can allow centralized programming control of the network 600, while managing and retaining all current in-store programming and functionally. The POS system 614 can manage data processing needs of the network 600, can store and allow modifications of vending machine settings, and can implement gathering and maintain marketing, customer survey and other informational databases. Further, POS system 614 can support transaction processing, and/or implement the universal server functionality.

Detailed Description Text (75):
Interconnected with a server 632 is the first LAN 622. A server 632 can be a system 500. In an exemplary embodiment, the server 632 can allow centralized programming control of the network 600, while managing and retaining all current in-store programming and functionally. The server 632 can manage data processing needs of the network 600, can store and allow modifications of vending machine settings, and can implement gathering and maintain marketing, customer survey and other informational databases. Also, server 632 can support transaction processing, and/or implement the universal server functionality.

Detailed Description Text (76):
Interconnected with a smart card re-value station 638 is the second LAN 626. A smart card re-value station can be a system 500. The smart card re-value station 638 can accept a valid form of ID, and/or currency. Furthermore, the smart card re-value station 638 can data communicate by way of the auxiliary terminal control means 530, to a smart card. Additionally, by way of the universal server and/or the dynamic identification interchange (DII) the smart card re-value station 638 can add or subtract value (monetary/credit/units) from a smart card. (The dynamic identification interchange is further disclosed in FIG. 11 in the transaction routing routine 900, block 908.) The smart card re-value station 638 can also display the available amount of value (monetary/credit/units) available and currently stored on, or accessible by the smart card. A user can also select an amount to operate on (credit/debit) by way of a keypad 540. Additionally, a user can select the amount to add, subtract, or transfer from the smart card and from other banking, credit accounts, or other databases by way of smart card re-value station 638 preprogramming, universal server settings, or other input means. In an exemplary embodiment, the smart card re-value station 638 can, by way of the universal server and/or the DII transfer funds to and from, or between account(s), bank account(s), credit bureau(s), or other databases. The accounts or databases can be on-site, off-site, and/or accessible by way of remote location 606, 616, 618, 634, 636, or network 600.

Detailed Description Text (79):
Interconnected with access control terminal 650 is the second LAN 626. Access control terminal 650 can be a system 500. In an exemplary embodiment, an access control terminal can be utilized to accept ID and grant access to secured areas. For a retail location that has a 24-hour access area, an access control terminal 650 can be used to allow the general public to present ID to be verified and to enter the secured area. Acceptable forms of identification can include a smart card, or a magnetic card (i.e. credit card, debit card, pre-paid, automated teller machine (ATM) or other bank or private issued card), hotel room key/card or other insertion type identifying devices. Additionally, biometric input such as handwriting, voice, finger, palm, hand, eye (iris scan) identification can also be an acceptable forms of ID.

Detailed Description Text (86):
Referring to FIG. 9A-9B, there is shown a customer transaction routine 700. Processing begins in block 702 where a "capture a transaction" command is initiated. A "capture a transaction" command is initiated when a customer/user (generally referred to as a user) inserts a valid form of ID. Valid forms of ID's can include a smart card, or a magnetic card (i.e. credit card, debit card, pre-paid, automated teller machine (ATM) or other bank or private issued card), hotel room key/card or other insertion type identifying devices. Additionally, biometric input such as hand writing voice, finger, palm, hand, eye (iris scan) identification can also be an acceptable forms of ID. Processing then moves to decision block 704.

Detailed Description Text (87):
Processing in decision block 704 determines if valid ID data was received (presented by the user) in response to a "capture a transaction" initiated command. If the resultant is in the affirmative, that is the user has presented valid ID and the data from the ID has been recorded, then processing moves to block 706. If the resultant is in the negative, that is no valid ID was presented, the processing is returned to the calling routine.

Detailed Description Text (88):
Processing in block 706 creates a transaction record based in part on the recorded ID data. Transaction processing can then proceed as programmed in several different formats. In a first transaction process a PMS/MIS or POS system can process the transaction data and determine the validity of the transaction to continue "approved" use or "denied" use of the vending equipment. Any suitable method of transaction verification can be employed including local or remote databases, credit bureaus, corporate accounts, in-store accounts, or very important person (VIP) memberships to name a few.

Detailed Description Text (89):
In a second transaction process, a server, such as a universal server can process the transaction data and determine the validity of the transaction to continue "approved" use or "denied" use of the vending equipment. Any suitable method of transaction verification can be employed including local or remote databases, credit bureaus, corporate accounts, in-store accounts, or very important person (VIP) memberships to name a few.

Detailed Description Text (90):
In a third transaction process, a PC 630 can be used to determine validity of the transaction to continue "approved" use or "denied" use of the vending equipment. Any suitable method of transaction verification can be employed including local or remote databases, credit bureaus, corporate accounts, in-store accounts, or very important person (VIP) memberships to name a few. In an exemplary embodiment, such a transaction processing method could effectuate the use of Internet based data connections, intranet, extranet, telecommunication line such as phone, ISDN, ADSL,

or VSAT satellite communications. The transaction processing can be transparent and undetectable to a user of PC 630.

Detailed Description Text (91):
When transaction processing is complete and a resultant of the transaction process is determined, processing moves to decision block 708. In decision block 708, a test is performed to determine if the use of the vending equipment has been authorized. If the resultant is in the affirmative, that is the resultant of the transaction processing is "approved," then processing moves to block 712. If the resultant of the transaction processing is in the negative, that is the resultant of the transaction processing is "declined," then processing moves to block 710.

Detailed Description Text (92):
Processing in block 710 informs the user that the transaction-processing attempt was "declined." Processing control is then returned to the calling routine.

Detailed Description Text (93):
Processing in block 712 informs the user the transaction processing was "approved" and enables the vending for use. During use, relevant marketing data, and advertisements can be displayed on the system 500 interconnected with the vending machine. Relevant marketing data can include current date and time, location, total sale amount; and where appropriate total copies, faxed pages, time used, PC usage, online usage, electronic commerce charges, total prints and other relevant marketing data. Processing then moves to block 714.

Detailed Description Text (98):
Processing in block 718 allows a user to purchase by electronic commerce, transaction items advertised and displayed on any system 500 or vending machine capable of displaying the advertisements. The electronic commerce transaction can be processed as previously disclosed in processing block 706. Processing then moves to decision block 720.

Detailed Description Text (101):
Processing in block 722 can re-authorize transaction data. The users can be prompted to present ID again or choose to allow the same transaction data to be reprocessed. Alternatively, a user can terminate a transaction. Should a user decide to present ID or give consent to a re-authorizing of previous transaction data, processing moves to block 706. If a user decides to terminate the transaction or the universal server or system 500 or vending machine decides to terminate the transaction, processing moves to block 726.

Detailed Description Text (102):
Processing in block 726 terminates a transaction by disabling the appropriate vending machines and printing a transaction receipt. Printing of a receipt can be optional or at the user's request. Processing then moves to block 728.

Detailed Description Text (105):
Through non-limiting example, reliance on a universal server to administer service responses to a plurality of systems 500 begins processing in block 802. The universal server is interconnected with a plurality of systems 500 and a plurality of vending machines by way of a first LAN 622 and/or a second LAN 626. In block 802 the universal server, PMS/MIS 620 or POS system 614, or PC 630 determines if a service condition has been requested by a system 500 or a vending machine connected to the network 600. Such service conditions can include out of supply, determination of a lengthy period of time without usage, inability to successfully complete a transaction, and inability to print a receipt. In addition, security alerts and other service conditions can be transmitted for processing. Processing then moves to block 804.

Detailed Description Text (113):

For example, when a system 500 detects that a transaction has concluded on a particular vending machine controlled by said system 500, a transaction complete service record can be sent to server 632. Server 632 in accordance with programming from a network administrator may store the record in a transaction database, and respond to the service request from the said system 500 by data communicating an acknowledge signal. A server 632 can be a universal server. Processing moves to block 810.

Detailed Description Text (115):
There is shown in FIG. 11, a transaction routing routine 900. Processing begins in decision block 902, wherein transaction data is evaluated to determine if it is PRE-VEND or POST-VEND transaction data. If the resultant is that the transaction data is PRE-VEND transaction data, that is the customer has not yet used the vending equipment for a product or service, processing moves to block 904. If the resultant is that the transaction data is POST-VEND transaction data, that is, the customer has previously been authorized to use the vending equipment and has now concluded the vending transaction, processing moves to block 914.

Detailed Description Text (116):
In block 904, any acceptable form of identification (ID) presented by a customer or other person in any system 500 connected to the first LAN 622 or the second LAN 626 is read/processed/measured/extracted/obtained or otherwise recorded. Acceptable forms of identification can include a smart card, or a magnetic card (i.e. credit card, debit card, prepaid, automated teller machine (ATM) or other bank or private issued card), hotel room key/card or other insertion type identifying devices. Additionally, biometric input such as handwriting, voice, finger, palm, hand, eye (iris scan) identification can also be an acceptable form of ID. For disclosure purposes, a first and second LAN 622 and 626 is generally referred to as a network 600. Processing then moves to block 906.

Detailed Description Text (118):
Processing in block 908 checks a routing table resident within the universal server. A routing table determines if a transaction "swap data step, append data step, convert data step, route data step, and/or process data step" is required. Said transaction "swap data step, append data step, convert data step, route data step, and/or process data step" processing is referred to as a dynamic identification interchange (DII). The DII process accepts a first identification form/transaction form and substitutes the first form for a second form. For example, a hotel room key/card may be accepted as a first form of ID and in a DII processing step substituted for or appended to a second form of ID, a credit card. This process can allow a user to have goods and services billed to a credit card by being identified first with a hotel room key/card. Processing then moves to block 910.

Detailed Description Text (120):
In another exemplary embodiment, a customer can present an ACCESS card (such as a smart card) as a first form of ID. The universal server can evaluate the ID form as presented and grant access to an unattended 24-hour access area. The same form of ID can then be presented in a variety of vending machines. Upon the presentation of the first form of ID in these vending machines the DII processing can substitute or append a second form of ID, an in-store account number. As the customer uses a plurality of vending machines for goods and services transaction billing can be posted to the in-store customer's account.

Detailed Description Text (121):
In another exemplary embodiment, a customer can present a first form of ID requesting to use a vending machine. Through DII processing it may be determined that the customer qualifies for special pricing, or has earned a promotional reward. The DII process step could substitute or append a second form of ID, such as a database record number to the transaction record. The database record number

could record the promotional reward status and further request a second DII processing step. This second DII processing step could append from a third data source relevant customer information (i.e. name and address). Any number of DII steps could be requested without limitation. The full transaction record could then be recorded in a database. Using this newly created data record, information could be mailed or the customer otherwise contacted with regards to the promotional reward. At the same time the DII processing is occurring, a service request can be initiated by calling service routine 800. With instructions from the DII settings, including pricing in the system 500 or vending machine the customer is being authorized to use, can be reprogrammed. Upon authorization approval, the vending machine and its performance will be custom programmed for this customer's use.

Detailed Description Text (122):
In another exemplary embodiment, a user presents a first form of ID and desires to use a PC 630. A DII processing step can send instructions to a server controlling a PC 630 or to a PC 630 directly. While the DII processing step is determining if a second form of ID is required and how the transaction should be routed, PC 630 reconfigures the desktop. In such a scenario, the user has been previously allowed to configure the PC 630 as desired to suit processing need and ease of use requirements. The DII step invokes in the PC 630, a reset function to access the user's established profile and reconfigures the PC 630 to the user's settings. In this fashion, a PC 630 user can travel to a PC 630 located in any location of the world and by way of a common network database, reconfigure the PC 630 to his or her preferences. In the scenario where there are thousands of franchised locations desiring to have PC's 630 in thousands of in-store and out-of-store locations, a user can present a first form of ID and have any PC 630 reconfigured to their personal preferences.

Detailed Description Text (123):
In another exemplary embodiment, a user can present a first form of ID at a PC 630. A DII processing step can determine the status of the user (number of previous visits, preferences) and prompt the user to answer customer survey questions. DII processing can route transaction information and customer survey responses to any desired location or database. Additionally, through DII processing, accounts can be established to allow an electronic commerce transaction to occur. Such accounts can include customer identification, customer purchasing history, customer credit limits, other customer information, electronic commerce accounts, payment accounts, shipping accounts, local franchise store locations, local in-store customer account information and other related account detail. Should a customer desire to purchase products through an electronic commerce transaction from a distribution fulfillment center ("DFC") located anywhere in the world, a DII processing step can effectuate the transaction. A distribution fulfillment center is any store, manufacturer, warehouse, or other repository of goods and or services from which a customer can purchase, ship, receive, and or order fulfill said goods and services. A pack and ship type company can be a distribution fulfillment center.

Detailed Description Text (124):
In addition, a DFC can initiate a transaction and use the DII processing to bill a customer who may have an account accessible by way of the present invention. Such DFC initiated transactions can be particularly useful for billing a group member, club member or customer with an association to a business, store, or group.

Detailed Description Text (125):
Any form of ID can be presented to a DII resident on or accessible by a universal server, resident in or accessible by a system 500, resident on or accessible by a vending machine, or resident in a database accessible by a universal server, system 500, or vending machine. If the transaction requires a DII processing step, the step can be performed transparent to the users or with the user's input. Furthermore, the DII can encrypt and decrypt transaction data, whereby secure transaction processing can be accomplished. DII processing can occur locally or

remotely worldwide.

Detailed Description Text (126):
Processing in block 910 invokes a routing routine to determine if a DII step is required and where the resultant transaction processing should be routed. Accordingly, a transaction can be DII processed, if necessary, and routed to a transaction processor. Such a transaction processor could be the in-store or hotel PMS/MIS or POS system. If the transaction is a credit card transaction that requires the step of "authorization," "sale," "settlement," or other credit card processing step, the hotel or retailer's PMS/MIS or POS system can complete the processing step. Should the PMS/MIS or POS system be unable to complete these types of transactions, the universal server, system 500 or other data processing device in a network 600 can complete these steps. Processing then moves to block 912.

Detailed Description Text (127):
In an exemplary embodiment, secured transaction processing referred to in block 910 can be by way of VISA/MASTERCARD Secure Electronic Transaction ("SET") protocol standard. Furthermore, SET transaction processing can be implemented by way of a system 500, a vending machine, or a universal server. The SET protocol standard for secured transaction processing can be implemented with other data processing equipment accessible by a system 500, vending machine or the universal server.

Detailed Description Text (128):
Processing in block 910 can effectuate the following exemplary embodiment. A customer can enter or check into at hotel or retail outlet, wherein a valid credit card is entered into the hotels or retailer's PMS/MIS system, or POS system. The customer can then be given an ID form, such as a card, smart card, hotel room key/card, or present another form of ID (biometric). This second form of ID can be entered into the hotel's or retailer's PMS/MIS or POS system. The customer can then present the second ID form to facilitate a vending transaction in any system 500. Transaction information by way of the network 600 can data communicate to the universal server transaction information to obtain first or other ID forms (such as payment or account ID forms). DII processing can then access the hotel's or retailer's PMS/MIS or POS system and obtain the customer's valid credit card or billing information. The credit card or billing data can be appended to the transaction record. The new appended transaction record can then be routed for processing. Transaction processing can include, but is not limited to adding the charges to a hotel bill (folio), paying cash, charging a smart card or credit card, charging an account, or recording the charges in a database.

Detailed Description Text (129):
Processing in block 912 routes PRE-VEND transactions for validation. Transaction validation can occur in a plurality of ways dependent on server programming, hotel/retail outlet preference, as well as based on card type, and/or ID type. Transactions can be validated at a remote location, such as remote location 616 whereby access to remote location 616 is by way of a system 500, network 600, and POS system 614. In addition, transactions can be validated at a remote location, such as remote location 618 whereby access to remote location 618 is by way of a system 500, network 600, and PMS/MIS system 620. Furthermore, transactions can be validated at a remote location, such as remote location 606 by way of a system 500, network 600, and PC 630. Transactions can also be validated at a remote location, such as remote location 634 whereby access to remote location 634 is by way of a system 500, network 600, and server 632. Server 632 is a universal server. Furthermore, transactions can be validated at a remote location, such as remote location 636 whereby access to remote location 636 is by way of a system 500. Additionally, transactions can be validated by way of a database resident in a system 500, a POS system 614, a server 632, or a PMS/MIS system 620. Transactions can also be validated by way of a database accessible by a system 500, a POS system 614, a server 632, a universal server, or a PMS/MIS system 620.

Detailed Description Text (130):
The resultant of the transaction processing is data communicated to the requesting system 500. If the resultant is in the affirmative, the customer is "approved" to use the vending equipment, then the requesting system 500 activates the vending equipment for use by the customer. If the resultant is in the negative, that is the customer has been "declined" for vending machine usage, then the requesting system 500 denies usage of the appropriate vending machine. The customer is notified of the "declined" status by way of LED indicator means 504, voice record and playback means 570, first display means 582, or other indicators means. Processing then moves back to the calling routine.

Detailed Description Text (131):
Processing in block 914 routes POST-VEND transaction data. POST-VEND transaction data includes PRE-VEND identification data, in addition to the marketing data generated resultant from the vend process.

Detailed Description Text (132):
Examples of PRE-VEND transaction data can include identification, date, time, appended ID data, sale limits, system pricing, merchant identification, routing codes, and system 500 ID codes. Additional PRE-VEND transaction data can include network traffic codes, authorizing sale amounts, system 500 configuration parameters, database access codes, remote location codes, currency codes, terminal codes, and other routing and system operational codes.

Detailed Description Text (133):
Examples of the marketing transaction data can include sale amount, finish date, finish time, total copies, total fax pages sent locally, total fax pages long distance, total fax pages sent internationally, and total fax pages received. System 500 and network programming control local, long distance, and international faxing delineation. Additional marketing transaction data can include total PC 630 general usage time, PC 630 applications utilized/usage time, PC 630 online usage (site contact specific, service specific, time used per site), total printed output count from a plurality of printers, and total scans made into the PC 630. Additional marketing data can include electronic commerce purchases, smart card re-valued totals, laptop usage, data port usage, and/or other marketing/transaction measurement/indicator data.

Detailed Description Text (134):
Routing of post-vend transaction processing by way of the DII is resultant from the updating of processing databases, accounting databases, and marketing databases in which the DII controls, manages, and/or has access to as shown in block 908. Further, post-vend transaction processing by way of the DII is resultant from post processing of credit cards, smart card and other types of transactions that require an intervening process to effectuate an electronic transfer of funds.

Detailed Description Text (135):
PRE-VEND and POST-VEND transactions can be processed by way of the PC 630 simultaneously and transparently to a user of the same PC 630. This functionality allows the PC 630 to be a vending machine interconnected with a system 500, a universal server such as server 632, PMS/MIS system 620 or a POS system 614. Furthermore, the PC 630 can implement the DII transaction processing as disclosed in block 908 and block 912. Additionally, the PC 630 can implement the DII locally with reliance on a remote site/server over a TCP/IP network, a Microsoft NT network, a Novell Netware network, an Internet connection, a VSAT connection, or other network interface. Also, the PC 630 can implement the DII residing remotely on a remote site/server over a TCP/IP network, a Microsoft NT network, a Novell Netware network, an Internet connection, a VSAT connection, or other network interface.

Detailed Description Text (144):

In block 1106, the universal server processes the data communication between the universal server, system 500 (containing the smart card), and any other device as necessary that is present on network 600. If required, the universal server can request a DII processing step to obtain appropriate or verify transaction data. Processing then moves to block 1108.

Detailed Description Text (145):
Processing in block 1108 is responsive to the resultant obtained from processing in block 1106. Furthermore, if a DII response requires additional information, processing in block 1108 prompts the user for such information/data. For example, a user can be prompted to enter, by way of keypad 540, the amount of money/units/credit to transfer to the smart card from sources acquired by the DII processing step. If additional data, such as the presentation of a credit card is required to effectuate the transfer of cash value, the customer can be prompted to "swipe" or otherwise present a valid credit card. If the universal server is able to utilize the DII to obtain data required to effectuate transaction processing, a customer may only be asked to "confirm-to-continue" with the transfer. In another exemplary embodiment, the re-valuing by way of the universal server, and/or DII processing can be seamless to the customer and transfers funds (money/credit/units) to the smart card without any intervention by the customer. Processing then moves to block 1110.

Detailed Description Text (146):
Processing in decision block 1110 effectuates the processing of the transaction and eventual "approval" or "denial" of a request to transfer funds (money/credit/units) to the smart card. If the resultant is in the negative, that is, the transaction has been "denied" then processing returns to the calling routine. If the resultant is in the affirmative, that is, the transaction has been "approved" then processing moves to block 1112.

Detailed Description Text (147):
Upon "approval" processing in block 1112 data communicates between the universal server, system 500 containing the smart card, and any other device (as required) on network 600 to effectuate the transfer of funds (money/credit/units), and subsequent transaction processing (billing "settling" as required). The transaction is then completed, prompting the users to facilitate any final actions as may be required. If the customer desires a receipt of the transaction just completed, a receipt can be printed by any printer on network 600. Processing control then returns to the calling routine.

Detailed Description Text (159):
There is shown in FIG. 15, an advertising routine 1300. Processing begins in block 1302 when a user presents a valid form of ID at a system 500 to begin a transaction. Alternatively, processing in block 1302 can begin by way of a person responding, with a keypad 540 or other system 500 data input, to an advertisement that may be displayed on a system 500 currently not in use.

Detailed Description Text (160):
In addition to the processing disclosed in transaction routine 900, the DII can select advertising and other marketing advertisements from a database (remote database or local database). The selection of marketing advertisements can be random or in accordance with a customer profile (individual or by group type). Customer profile parameters can be accessible by the universal server and/or by way of DII process steps.

Detailed Description Text (165):
Processing in block 1308 adds the amount of an electronic commerce purchase to the total of the current transaction. If the customer/user interacted with a system 500 in which no current transaction was in progress, the system 500 by way of the universal server will prompt the user to present a valid form of ID and start a

transaction. DII processing, can be relied upon to associate any form of valid ID presented to facilitate the electronic commerce purchase. Receipts or other printed documents, such as order forms or conformation forms can be printed on a printer on network 600 as required. Processing control is then returned to the call procedure.

Detailed Description Text (166):
There is shown in FIG. 16, a print routine 1400. Processing begins in block 1402 when a system 500 desires to print data on a printer, such as printer 612A or printer 612B. In an exemplary embodiment, print data can be advertisement print data, transaction summary print data, receipt print data, vending machine print data, such as from a PC 630, or other print data. If a system 500 is preprogrammed with a network 600 network location ID (network address) for a printer 612A or 612B, then printing on printer 612A or 612B can be facilitated by way of a data communication between the system 500 and printer 612A or printer 612B. Subsequent to any printing, a data communication between the system 500 desiring to print and the universal server can occur, wherein the system 500 desiring to print data requests permission from the universal server to data communicate print data to printer 612A or 612B. If permission is granted and printing is successful, processing control returns to the calling procedure. If processing is not successful, then processing moves to block 1404.

Detailed Description Text (171):
There is shown in FIG. 17, a POST-VEND transaction processing routine 1500. Processing begins in block 1502, wherein a POST-VEND transaction is data communicated to the universal server. Processing then moves to block 1504.

Detailed Description Text (172):
In block 1504, the universal server, by way of DII processing (as required) routes the POST-VEND transaction for payment, posting, or billing. The process of payment, posting or billing is generally referred to as "settling" or a "settlement" transaction. Transactions can be routed based on transaction type (credit card, smart card, pre-paid card, hotel key/card, or biometric) to different remote locations, or to different on-site or off-site databases. Furthermore, post-vend transactions can be routed based upon preprogrammed criteria. For example, all credit card transactions requiring "settlement" can be routed to a first credit bureau until a certain gross daily, monthly, annual dollar amount is achieved. Once the preprogrammed criterion has been satisfied credit card transactions requiring "settlement" can then be routed to a second credit bureau. Processing then moves to block 1506.

Detailed Description Text (173):
In block 1506, non-credit card and POST-VEND transactions not requiring any additional third party port processing (i.e. by way of a credit bureau) are "settled" by posting the POST-VEND transaction data, by way of DII processing (as required) to the appropriate remote location, or on-site or off-site database. The universal server can be preprogrammed to store POST-VEND transactions and "batch" post transaction data based on a preprogrammed criteria. Such "batch" posting preprogrammed criteria can be based in part on date, time, or quantity of transactions, transaction dollar amount, availability of the database or remote location, or other cost, performance or preferences. The term "batch" processing is defined as the process of posting any number of transactions at once in a formatted block of data. Processing then moves to block 1508.

Detailed Description Text (174):
In block 1508, POST-VEND transactions reliant on a third party processor (i.e. credit cards) are processed in accordance with preprogramming of the universal server. Preprogramming of the universal server can include processes and procedures disclosed in block 1504, and 1506. Processing then moves to block 1510.

Detailed Description Text (175):
In block 1510, the universal server determines whether the POST-VEND transaction processing was successful. If the POST-VEND transaction processing was not successful, that is, the universal server was unable to post process the POST-VEND transaction, then the universal server can data communicate the "unsettled" post vend transaction to a remote locate. Such a remote location can be a computer center that monitors the functionality of a plurality of universal servers. The remote location can be remote location 606, 616, 618, 634, or 636. Processing control is then returned to the calling procedure.

CLAIMS:

1. A public access electronic commerce system for controlling access to a computer network and usage of a personal computer, comprising: a computer network interface linked to said personal computer and said computer network; a public access electronic commerce terminal connected to said personal computer, said public access electronic commerce terminal including: identification means for i) accepting at least one of a plurality of identification inputs from a user and ii) effectuating selectively a dynamic identification interchange of said at least one of a plurality of identification inputs from said user, to effectuate payment or transaction processing and for controlling access to said personal computer and said computer network, and means for determining a non-use period of said public access electronic commerce terminal; a universal server connected to said computer network, said universal server including: a plurality of data regarding a plurality of users stored therein, means for communicating a plurality of satisfying criteria to said public access electronic commerce terminal, said satisfying criteria including a plurality of data regarding an ability to pay for usage of said personal computer and said computer network by said user, means for recording user usage of said personal computer and or said computer network, and means for transmitting said user usage to another universal server; means for generating an error condition of said public access electronic commerce terminal based on an output of said non-use determining means; means for determining if at least one of a system limit and an authorization limit of said user is at least one of reached and exceeded; means for reauthorizing said user based on an output of said determining means; and means for reprocessing said user usage based on said reauthorization.

2. An operationally controlled data-port connection in accordance with claim 1, wherein said a plurality of software operating on a PC is a transaction control device.

14. The system in accordance with claims 13 wherein, said plurality of other computing devices includes a hand-held personal digital assistant.

36. A public access electronic commerce system for controlling access to a computer network and usage of a personal computer, comprising: a computer network interface linked to said personal computer and a computer network; a public access electronic commerce terminal coupled to said personal computer, said public access electronic commerce terminal including: a) identification means for accepting at least one of a plurality of identification inputs from a user and for effectuating a selective dynamic identification interchange of said at least one of said plurality of identification inputs, to effectuate payment or transaction processing for access to said computer network and usage of said personal computer, and for controlling access to said personal computer and said computer network based on said dynamic identification interchange, and b) means for determining a non-use period of said public access electronic commerce terminal; a universal server connected to said computer network, said universal server including: a plurality of data regarding a plurality of users stored therein, means for recording user usage of said personal computer and or said computer network; means for transmitting said user usage to another universal server; means for generating an error condition of said public

access electronic commerce terminal based on an output of said non-use determining means; means for determining if at least one of a system limit and an authorization limit of said user is at least one of reached and exceeded; means for reauthorizing said user based on an output of said determining means; and means for reprocessing said user usage based on said reauthorization.

Previous Doc Next Doc Go to Doc#

L14: Entry 741 of 792 File: USPT Oct 23, 2001

DOCUMENT-IDENTIFIER: US 6305603 B1
** See image for Certificate of Correction **
TITLE: Personal digital assistant based financial transaction method and system

Abstract Text (1):
A personal digital assistant (PDA) based financial transaction method and system. The invention allows for convenient access to financial account(s) from a store and allows for financial transactions and immediate account updates via a PDA.

Brief Summary Text (3):
The present invention relates generally to financial electronic transactions and, in particular, to convenient electronic financial transactions and financial account(s) access with immediate account updates via a personal digital assistant (PDA).

Brief Summary Text (5):
Heretofore, credit cards, automated teller machine (hereafter"ATM"cards and so called smart cards have been used to purchase products and services without the use of cash. Unfortunately, the before mentioned cards suffer from a number of disadvantages. First, they do not provide the ability to use multiple accounts to pay for a transaction. Second, some cards such as credit cards or smart cards do not require an electronic signature or password for access to a users account. Hence, if lost or stolen, the card holders assets can be lost. Third, the above-mentioned cards do not provide feedback for record keeping other than a purchase receipt. The card user, therefore, must remember to enter the amount of purchases into his/her account register and update the account balance. Balance maintenance and budgeting, therefore, are burdensome.

Brief Summary Text (6):
In view of the foregoing, there is a need for a process and system(s) for conveniently conducting multiple financial transactions and automatically updating accounts.

Brief Summary Text (8):
In a first general aspect of the present invention is provided a method comprising the steps of: accessing at least two financial accounts at at least one financial institution using a personal digital assistant, performing at least one financial transaction during accessing using the personal digital assistant, and transmitting from each financial institution to the personal digital assistant updated information regarding each financial account. The present invention provides a number of advantages over related art devices. First, the process allows access to accounts with immediate updated feedback from the financial institution(s) accessed. This allows the user to access more than one account at one time if necessary and immediately see updated account balances on the personal digital assistant. Hence, the user receives more accurate account information. Additionally, prior to proceeding with a financial transaction, the PDA user may be provided with current financial account information so as to prevent overdrafts and allow for budgeting. Another advantage is found in how the retail institution or other transaction processor would receive immediate payment for goods or services, and potentially without providing a check out clerk or other service

representative. Payment would be provided automatically by the PDA user before exiting the store. Accordingly, usage of the present invention could ultimately lead to lower costs to a transaction processor.

Brief Summary Text (9):
In a second general aspect in accordance with the present invention is provided a financial transaction system comprising: a hand held microcomputer electronically communicative with a store computer, the store computer being electronically communicative with at least one financial institution computer. The system further includes means for executing an electronic financial transaction between at least one hand held microcomputer user account at the at least one financial institution and a store account, and for immediately updating account information on the hand held microcomputer after the electronic financial transaction has been completed. This aspect provides a system to carry out the process of the first aspect and provides all of the advantages outlined above.

Brief Summary Text (10):
A third general aspect of the present invention provides a system for performing a financial transaction at a store, the system comprising: a store computer communicative with a store financial institution computer and a hand held computer user financial institution computer. The hand held computer has means for communicating with the store computer, means for initiating a financial transaction between the hand held computer user financial institution and the store financial institution computer via the store computer, and means for receiving financial transaction and account details from the hand held computer user financial institution computer via the store computer. This aspect provides similar advantages as that of the second aspect.

Brief Summary Text (11):
A fourth general aspect of the invention provides a store computer system for performing a financial transaction at a store with a hand held computer, the system comprising: means for communicating with a financial institution of the store and with a financial institution of the hand held computer user, means for communicating with, and performing a financial transaction based on input from, the hand held computer, and means for transmitting financial transaction and updated financial account information from the financial institution of the hand held computer user to the hand held computer. This aspect provides a store system capable of obtaining the above-described advantages.

Brief Summary Text (12):
A fifth general aspect of present invention provides a program storage device readable,by a machine, tangibly embodying a program of instructions executable by the machine to perform the method steps for executing a financial transactions between computer systems, the method steps comprising: accessing at least two financial accounts at at least one financial institution using a personal digital assistant, performing at least one financial transaction during accessing using the personal digital assistant, and transmitting from each financial institution to the personal digital assistant updated information regarding each financial account. This aspect provides a mechanism of storage for instructions to carry out the process outlined above.

Detailed Description Text (3):
A"personal digital assistant" (hereinafter"PDA") is defined as a hand held microcomputer designed for individual use and includes at least a local central processing unit (CPU), a touch screen (or other equivalent user interface such as a keypad, a screen with mouse, voice recognition system, or pen-based input, etc.), memory for storing information, and input/output capability for reading and writing information. The I/O capability may be to various cards such as smart cards, magnetic cards, or optical cards, etc. The PDA may also include a microphone, a modem, a serial port and/or a parallel port so as to provide direct communication

capability with peripheral devices, e.g., point of sale (POS) and automated teller machine (ATM) terminals, and capability for transmitting or receiving information through wireless communications such as radio frequency (RF) and infrared (IR) communications. Examples of such devices are an International Business Machine (IBM) Workpad.RTM. or an Apple Newton.RTM..

Detailed Description Text (5):
A"transaction processor" or"store" is any establishment in which a person pays for products, services, etc. It is important to recognize that while the term"store" is used throughout to describe the subject invention, the teachings of the invention, as they relate to an establishment receiving payment, are applicable to any establishment that receives payment and should not be limited to a traditionally defined"store." For instance, internet commerce, websites, ATM machines, stock markets or brokers, car rental companies, etc. are all considered "transaction processors" or"stores." In some instances, the establishment may be both a store and a financial institution, e.g., stock brokers.

Detailed Description Text (6):
Referring to FIG. 1, a representative hardware environment for practicing the present invention is depicted that illustrates a typical hardware configuration of a PDA based financial transaction system in accordance with the subject invention. The system includes a personal digital assistant (PDA) 10 such as an IBM Workpad.RTM.. PDA 10 is communicative via mechanism 12 to a transaction processor's or store's computer system 20 and, in particular, to any one of a number of communication ports or kiosks 14A, 14B, 14C, 14D, 14E, etc. that may be positioned anywhere throughout a store. Communication mechanism 12 can take a variety of forms that allow electronic communication. For instance, wiring. If PDA 10 has wireless communication capabilities, then communication mechanism 12 may include a compatible receiver/transmitter 16, e.g., an infra-red data communication port.

Detailed Description Text (7):
Store computer system 20 would include a CPU, ROM, RAM and assorted input/output devices. Store computer system 20 would also include networked kiosks 14A-14E. Store computer system 20 can also electronically connect, e.g., via modem or wide area system, to any number of financial institution computer systems 30, 32, 34 in which the PDA user and/or store has at least one account.

Detailed Description Text (8):
Turning to FIGS. 2-3, the overall processes involved with the present invention are illustrated. In step S1 of FIG. 2, PDA 10 initiates payment transfer at a conveniently located kiosk 14A-14E in the store. That is, PDA 10 is electronically communicative with store computer system 20 via wired or wireless communication via kiosk 14A-14E. At this point, payment information such as the cost of the product or services is entered. This information may be inputted into either PDA 10, or store computer system 20 directly via kiosk 14A-14E, in a number of ways. For instance, the price can be entered via a keyboard or more preferably via conventional bar code reader scanning. Once a final financial transaction total has been obtained, it is reported to the PDA 10 user, i.e., if inputted into a kiosk 14A-14E, kiosk 14A-14E transfers the transaction amount to PDA 10.

Detailed Description Text (9):
In step S2, the PDA user chooses the financial account or accounts and amount to debit from each to cover the amount of the financial transaction. The financial account(s) can be at a single financial institution or a number of financial institutions. The selections would be presented on the output device of PDA 10 and selectable by the user as desired. For instance, PDA 10 may include a touch screen, a screen with mouse, a pen-based system, a keypad, or voice recognition system, etc., for item selection by the user. Input of amounts to be debited to each financial account could be provided with the same selection mechanisms.

Detailed Description Text (10):
In step S3, a determination as to whether the financial transaction amount has been covered by the selections is performed. If the transaction is incomplete, the process loops until selections are made by the PDA user to cover the total amount of the financial transaction. If the final transaction total has been covered by the selections, the process proceeds to step S4 where a user enters an account access approval indication such as passwords, personal identification numbers (PIN), voice recognition approval, etc., for each account selected to be debited. The store may also have in memory an account access approval indication for each of its accounts that would be accessed for transfer to the respective financial institution.

Detailed Description Text (11):
In step S5, account accessing and communication processes with financial institution computer system(s) 30, 32, 34, etc. by an executing computer system, are illustrated. The financial institution computer systems 30, 32, 34, etc. access is determined, in part, by which financial institution accounts the PDA user designates to be debited and also by which financial institution accounts the store designates to access. For example, if the store and PDA user have accounts at the same financial institution, a minimum of two accounts will be accessed, or if the store and PDA user each designate more than one account at more than one financial institution, a minimum of four accounts may be accessed. Communication with each financial institution is to be in parallel such that simultaneous electronic financial transactions can occur. It is important to note, however, that membership in standardized financial transaction programs, e.g., CIRRUS.RTM., MAC.RTM., NYCE.RTM., etc., could reduce the necessary number of financial institutions accessed.

Detailed Description Text (12):
The executing computer system may be either store computer system 20, PDA 10 or financial institute computer 30, 32, 34, etc., i.e., software execution for the actual financial transaction may take place in any system. Preferably, however, the executing computer system would be either financial institute computer system 30, 32, 34, etc. or store computer system 20 based on their probable higher storage capacity and performance parameters as compared to PDA 10. Most preferably, store computer system 20 is the executing computer system.

Detailed Description Text (13):
Referring to FIG. 3, the details of step S5 are illustrated. At step S6, financial institution computer system 30, 32, 34 receives a request for transaction from the executing computer system, e.g., PDA 10 or store computer system 20. This request (s) would include the inputted account access approval indications for each account to be accessed. As is conventional, all information communicated is encrypted. For instance, a 128 bit encryption key, dynamic encryption system (DES), etc. can be used to assure security. Alternatively, a secure virtual private network system (VPN) is also possible.

Detailed Description Text (14):
In step S7, financial institution computer system(s) 30, 32, 34 receive encryption keys from PDA 10 and store computer system 20. In step S8, the encryption keys are returned or transmitted to PDA 10 and store computer system 20.

Detailed Description Text (15):
In step S9, the current account(s) information is transmitted to PDA 10. This information advantageously would include at least current account(s) balance(s) and possibly all past transactions, i.e., account transaction history, which may or may not have been recorded by the PDA user. If account transaction history is desired, the number of days, weeks, months, etc. of history to be obtained can be set by the PDA user. Hence, the user can be apprized of current account balances and, if desired, determine paper transactions that have not yet cleared by reviewing the

account transaction history. These provisions allow the PDA user to have the most up to date information before completing any final transactions. In a preferred embodiment, PDA 10 includes a financial account tracking database that is used to maintain and track financial accounts activity and balances. This database would be updated by the current account(s) information. However, it is also possible that at the PDA user's choosing (e.g., for security reasons), PDA 10 would not have information stored thereon and all account information would be transferred from the financial institution(s) upon use. In this case, PDA 10 would act as a terminal. Information regarding a store account(s) can also be sent to store computer system 20, if desired.

Detailed Description Text (16):
In step S10, the encrypted transaction parameters are received by financial institution computer system(s) 30, 32, 34. Transaction parameters may include, for example, transaction amount, account information, type of transaction (e.g., debit, transfer, credit), etc. Further, for some transactions, such as those requiring financial status verification (e.g., mortgages, car loans, etc.), other PDA user account information could be transferred to the store.

Detailed Description Text (17):
In step S11, a return commit request is sent to PDA 10 for a two-step or two-phase transaction committal from the PDA user. It should be recognized that the committal does not necessarily have to require two phases and may take the form of any committal indication desired by the PDA user, store and/or financial institution. For instance, a password or PIN, voice recognition, handwriting recognition, alphanumeric signal, etc. can be used.

Detailed Description Text (18):
In step S12, the financial transaction is performed. More specifically, the committal confirmation from PDA 10 is received and the financial transaction is performed. That is, the amount(s) selected from each financial account(s) of the PDA user to cover the amount of the financial transaction is transferred to the designated store account(s).

Detailed Description Text (19):
Next, in step S13, a transmittal from each financial institution to PDA 10 of updated information regarding each financial account is provided. In particular, a completed transaction notification is sent back to PDA 10 with the current account (s) information of the PDA user. After step S13, connection between store computer system 20 and the financial institution computer system(s) 30, 32, 34 can be discontinued.

Detailed Description Text (20):
Returning to FIG. 2, the overall process continues with step S14 where current account(s) information is transferred back to PDA 10 via store computer system 20 connection with PDA 10, assuming store computer system 20 is the executing computer. Otherwise, current account(s) information is sent directly to PDA 10. In step S15, the account(s) information is displayed on PDA 10 and the financial transaction is applied to a PDA database to update its records if PDA 10 has such capabilities. Hence, an automatic account register can be created. In step S16, the PDA user is queried as to whether more transactions are desired. If yes, the system loops back to step S2. Otherwise, the process is completed.

Detailed Description Text (21):
As an additional last step (not shown), an encrypted receipt could be sent to PDA 10 for further record keeping and presentation to a store representative prior to departure. As an alternative, a receipt could also be printed at kiosks 14A-14E for presentation to a store representative upon departure or at a pick up area within the store.

Detailed Description Text (22):
The method and process of the subject invention allow access to financial account (s) with immediate updated feedback from the financial institution(s) accessed. This allows the user to access one account or more than one account at one time, if necessary, and immediately see updated account balances on PDA 10. For example, if a user were buying a $1000 television, $500 could be debited to a checking account, $200 to a savings account, and $300 to a Visa account simultaneously. The balances of each account would be presented to the PDA user prior to completion of the transactions and after completion of the transactions. The user therefore receives more accurate account information. Additionally, prior to proceeding with a financial transaction, the PDA user is provided with current financial account information so as to prevent overdrafts. A transaction processor or store, such as a retail institution, would receive immediate payment for goods or services. Further, the transaction processor or store could potentially eliminate the need for checkout clerks or other service representatives other than someone to check receipts of a PDA user upon departure from the store. Alternatively, paper receipts could be eliminated entirely, for example, by providing an electronic receipt displayed on the PDA for presentation to a store representative upon departure. Hence, the subject invention could drastically decrease store operation costs.

Detailed Description Text (24):
For instance, the invention can be implemented as set(s) of instructions (i.e., a software program) resident in the read only memory (ROM) of the executing computer system, e.g., PDA 10, store computer system 20 or financial institution computer system 30, 32, 34, etc. Alternatively, the set of instructions can be segmented between computer systems 10, 20, 30, etc. as necessary.

Detailed Description Text (25):
Until required, the set of instructions may also be stored in another computer readable memory, for example in a hard disk drive, or in a removable memory such as an optical disk for eventual use in a CD-ROM drive or a floppy disk for eventual use in a floppy disk drive. Further, the set of instructions can be stored in the memory of another computer and transmitted over a local area system or a wide area system, such as the Internet, when desired by the user. For instance, the set(s) of instructions may be stored in financial institution computer system(s) 30, 32, 34, etc. If the Internet is used, the set(s) of instructions can be transferred directly to the executing computer system, i.e., PDA 10 or store computer system 20, as necessary. One skilled in the art would appreciate that the physical storage of the set(s) of instructions physically changes the medium upon which it is stored electrically, magnetically, or chemically so that the medium carries computer readable information.

Detailed Description Text (26):
Furthermore, the teachings of the present invention of immediately updating a PDA financial account database after a financial transaction may be applied in circumstances other than a debiting-type financial transaction without limitations. For instance, the present invention may be used for account transfers, e.g., transferring more funds between accounts or to a smart card. Transfers could occur prior to a debiting financial transaction, e.g., after the PDA user receives the current account information, or without a debiting financial transaction occurring. Further, the present invention could be used for situations where the establishment is both a financial institution and store as defined herein, e.g., a sale of stock by the PDA user, with transfer of proceeds to other accounts at the stock brokers or elsewhere.

CLAIMS:

1. A method comprising the steps of:

identifying a product to be purchased;

accessing at least two financial accounts, each of the accounts having at least one of funds and credit for the purchase of the product, at at least one financial institution using a personal digital assistant;

performing at least one financial transaction during accessing using the personal digital assistant; and

transmitting from each financial institution to the personal digital assistant updated information regarding each financial account.

2. The method of claim 1, further comprising:

entering into a store computer a price that a buyer will pay to purchase the product;

automatically providing to the buyer a receipt for the payment of the Price, said providing of the receipt being performed after the at least one financial transaction has been completed and being not performed by a human; and

releasing the product to the buyer if the buyer presents such receipt upon removal of the product from the store.

3. The method of claim 1, wherein the step of accessing includes transmitting an account access approval indication to the at least one financial institution for each account from the personal digital assistant.

6. The method of claim 1, further comprising the step of displaying the updated information for each account on the personal digital assistant.

7. The method of claim 1, wherein the step of accessing includes the personal digital assistant communicating with the financial institution via a store computer system.

8. The method of claim 7, wherein the step of transmitting includes transmitting the updated information to the personal digital assistant via the store computer system.

9. The method of claim 2, further comprising the step of entering a transaction amount into one of the personal digital assistant and the store computer system, wherein the transaction amount includes the price the buyer will pay for the product.

12. The method of claim 9, wherein the step of accessing includes transmitting from the financial Institution to the personal digital assistant at least one of, current account balances account transaction history and information for updating a database of the personal digital.

13. The method of claim 1, wherein the step of performing a financial transaction includes transferring a transaction amount to a store account.

16. The method of claim 1, wherein the step of accessing a financial account requires at least one transaction approval indication from the personal digital assistant.

17. A financial transaction system comprising:

a hand held microcomputer electronically communicative with a store computer, the store computer being electronically communicative with at least one financial institution computer;

means for executing at least two simultaneous electronic financial transactions between at least two financial accounts of the user of the hand held microcomputer at the at least one financial institution and a store account, and for immediately providing the hand held microcomputer with updated account information after the electronic financial transactions have been completed for each account.

18. A system for performing a financial transaction at a store, the system comprising:

a) a store computer communicative with a store financial institution computer and a hand held computer user financial institution computer; and

b) a hand held computer having:

i) means for communicating with the store computer;

ii) means for initiating a financial transaction between the hand held computer user financial institution and the store financial institution computer via the store computer; and

iii) means for receiving financial transaction and account details from the hand held computer user financial institution computer via the store computer;

means for automatically providing to the user an encrypted receipt recording the financial transaction and for presentation by the user upon removal of a product from the store.

19. A store computer system for performing a financial transaction at a store with a hand held computer, the system comprising:

means for communicating with a financial institution of the store and with at least one financial institution of the hand held computer user;

means for communicating with, and for performing at least two approximately simultaneous electronic financial transactions between at least two financial accounts of the user of the hand held computer at the at least one financial institution and a store account based on input from, the hand held computer; and

means for transmitting financial transaction and updated financial account information from the financial institution of the hand held computer user to the hand held computer.

20. A program storage device readable by a machine, tangibly embodying a program of instructions executable by the machine to perform the method steps for executing a financial transactions between computer systems, the method steps comprising:

a) accessing at least two financial accounts of a user of a personal digital assistant and a store account at at least one financial institution using the personal digital assistant;

b) performing at least one financial transaction during accessing using the personal digital assistant; and

c) transmitting from each financial institution to the personal digital assistant updated information regarding each financial account.

21. The method of claim 1, wherein the receipt provided to the buyer is an electronic receipt displayed on the PDA for presentation to a store representative upon the buyer's departure from the store.

Previous Doc Next Doc Go to Doc#

L24: Entry 21 of 21 File: USPT Jun 29, 1999

DOCUMENT-IDENTIFIER: US 5917913 A
TITLE: Portable electronic authorization devices and methods therefor

Abstract Text (1):
A portable electronic authorization device for approving a transaction request originated from an electronic transaction system. The portable electronic authorization device includes first logic circuit configured to receive first digital data representative of the transaction request. There is further included second logic circuit configured to form second digital data responsive to the transaction request received by the first logic circuit if the transaction request is approved by a user of the portable electronic transaction device. The second digital data represents encrypted data signifying an approval by the user of the transaction request. Additionally, the portable electronic authorization device includes transmission circuitry coupled to the second logic circuit. The transmission circuitry is configured to transmit the second digital data from the portable electronic authorization apparatus to the electronic transaction system if the user approves the transaction request.

Brief Summary Text (2):
The present invention relates to methods and apparatus for conducting electronic transactions. More particularly, the present invention relates to portable electronic authorization devices (PEADs) which advantageously and substantially eliminate the security risks associated with prior art techniques of approving transactions between a user and an electronic transaction system.

Brief Summary Text (3):
Electronic transaction systems are known. An electronic transaction system typically permits a user to conduct designated transactions electronically, which substantially improves efficiency and convenience to the user. Examples of electronic transactions include transactions conducted via computer networks, automated teller machines (ATM's), automated point-of-sale systems, automated library systems, and the like. Transactions conducted via computer networks may encompass a wide range of transactions, including exchanging information and data via a computer network popularly known as the Internet, e.g., to make a purchase from a vendor on the network. ATM's typically permit users to conduct financial transactions (such as withdrawals, transfers, deposits, and the like) vis-a-vis a financial institution in an electronic manner. Automated point-of-sale systems may be employed by merchants to permit users to purchase products or services using the users' electronic account, and automated library systems may be employed to permit library users to check out and return library materials. Other examples of electronic transaction systems are readily available in popular literature and are not enumerated herein for brevity sake.

Brief Summary Text (4):
To enhance security to the user's account, electronic transaction systems typically request the user to provide identification data to authenticate himself as the user authorized to approve the proposed transaction or transactions. If the user fails to provide the requested identification data, the proposed transaction or

transactions are not authorized and will not be processed. The identification data may be required with each transaction. By way of example, an automated point-of-sale system may require the user to approve a purchase transaction and will accept an approval message only if it is satisfied that the person approving the transaction has furnished adequate identifying data authenticating himself as the person authorized to perform the approval. Alternatively, the identification data may be entered by the user at the start of a session to authenticate himself and enable that user to subsequently perform any number of transactions without further authentication.

Brief Summary Text (5):
In the prior art, users are typically required to manually enter the identification data into the electronic transaction system for authentication. Typically, the entry of identification data involves typing in a password on a numeric keypad or on a keyboard. The identification data is then compared with data previously stored within the electronic transaction system, and authentication is satisfied when there is a match. As mentioned previously, the transaction or transactions proposed will not be allowed to proceed if there is no match.

Brief Summary Text (6):
Although prior art electronic transaction systems provide some protection from unauthorized access and use of the user's account, there are disadvantages. To illustrate certain disadvantages associated with prior art electronic transaction systems, reference may be made to FIG. 1 herein. FIG. 1 shows an automated teller machine (ATM) 100, representing the requesting device of an electronic transaction system 102. Electronic transaction system 102 may include, for example, a central database 104 which contains previously-stored identification data and account data of user 106.

Brief Summary Text (7):
To initiate a typical transaction with ATM 100, user 106 first inserts a data card 107, such as a bank card or a credit card, into a card reader 109. Data card 107 typically includes a magnetic stripe that contains the account number and other information related to the user, which may then be read by card reader 109. The data stored in data card 107 enables electronic transaction system 102 to ascertain which account in database 104 user 106 wishes to transact business.

Brief Summary Text (8):
Via a keypad 108 on ATM 100, user 106 may then be able to enter his identification data, e.g., his personal identification number (PIN), to authenticate himself. If the entered identification data matches the identification data stored with the account in database 104 that is identified by data card 107, the user is authenticated and granted access to his account. If there is no match, authentication fails. After authentication, user 106 may be able to, for example, employ a combination of keypad 108 and a screen 110 to withdraw cash from his account, which results in cash being dispensed from ATM 100 and the balance in his account within database 104 correspondingly reduced.

Brief Summary Text (9):
Theoretically, the identification data entered into ATM 100 should be secure. In reality, there are many potential security risks to the identification data in prior art authentication techniques. Since the identification data is not encrypted before being entered into ATM 100, the non-encrypted identification data is vulnerable to unauthorized access and procurement. Encryption of the identification data is not practical in the prior art since it would have been too complicated and/or inconvenient for the user to perform encryption or memorize the encrypted identification data. Unauthorized procurement of the identification data in the prior art may occur, for example, upon entry if it is inadvertently seen by another party, e.g., by another person behind user 106, either on screen 110 or more likely at keypad 108.

Brief Summary Text (10):
Even if encryption is employed on the identification data in the prior art, e.g., prior to transmission from ATM 100 to database 104, the encryption typically occurs within ATM 100 and still requires the entry of non-encrypted identification data from user 106 and the existence of the identification data for some duration of time in ATM 100. Unauthorized access to the identification data may then occur if an unauthorized party is able to gain entry into ATM 100 and intercepts, e.g., via software or hardware implemented in ATM 100, the non-encrypted identification data therein.

Brief Summary Text (11):
Furthermore, if public key cryptography is employed within ATM 100, the storage of the user's private key within ATM 100 renders this private key vulnerable to theft, further exposing the user's account to risk. The stolen password and/or private key may then be employed to allow unauthorized persons to access the user's account to the user's detriment.

Brief Summary Text (12):
In view of the foregoing, there are desired apparatus and methods for conducting transactions with the electronic transaction system while substantially eliminate the risk of unauthorized access to the user's account and unauthorized procurement of the user identification data. Preferably, such an apparatus should be easily portable to permit the user to conveniently and comfortably perform transaction authentication anywhere.

Brief Summary Text (14):
The present invention relates, in one embodiment, to a method in a portable electronic authorization device for approving a transaction request originated from an electronic transaction system. The method includes receiving at the portable electronic authorization device first digital data, the first digital data representing the transaction request. The method further includes transmitting a second digital data to the electronic transaction system if the transaction request is approved by a user of the portable electronic authorization device. The second digital data is encrypted by circuitries within the portable electronic authorization device and signifies the user's approval of the transaction request.

Brief Summary Text (15):
In another embodiment, the invention relates to a portable electronic authorization device for approving a transaction request originated from an electronic transaction system. The inventive portable electronic authorization device includes first logic circuit configured to receive first digital data representative of the transaction request. There is further included second logic circuit configured to form second digital data responsive to the transaction request received by the first logic circuit if the transaction request is approved by a user of the portable electronic transaction device. The second digital data represents encrypted data signifying an approval by the user of the transaction request. Additionally, the inventive portable electronic authorization device includes transmission circuitry coupled to the second logic circuit. The transmission circuitry is configured to transmit the second digital data from the portable electronic authorization apparatus to the electronic transaction system if the user approves the transaction request.

Drawing Description Text (3):
FIG. 1 shows a prior art electronic transaction system, including an automated teller machine (AMT).

Drawing Description Text (4):
FIG. 2 illustrates, in accordance with one embodiment of the present invention, a portable electronic authorization device (PEAD), representing the apparatus for

securely approving transactions conducted vis-a-vis an electronic transaction system.

Drawing Description Text (6):
FIG. 3B shows, in one embodiment, the format of representative transaction approval data.

Drawing Description Text (14):
FIG. 8 is a flowchart illustrating, in accordance with one aspect of the present invention, steps involved in encrypting transaction approval data using a public key cryptography technique.

Detailed Description Text (2):
FIG. 2 illustrates, in accordance with one embodiment of the present invention, a portable electronic authorization device (PEAD) 200, representing the apparatus for securely approving transactions conducted vis-a-vis an electronic transaction system. With reference to FIG. 2, requesting device 202 may initiate a transaction approval process with PEAD 200 by transmitting to PEAD 200, via communication port 204, a transaction request pertaining to a proposed transaction. Requesting device 202 may represent, for example, an ATM machine, a computer terminal in a network, an automated library check-out terminal, or similar devices for permitting the user to transact business with the electronic transaction system. The proposed transaction may be, for example, a sale transaction of a particular item for a certain amount of money. The transaction request itself may include, for example, the transaction ID, the merchant's name, the merchant's ID, the time of the proposed purchase, and the like. In one embodiment, the transaction request from requesting device 202 may be encrypted for enhanced security but this is not required. Data pertaining to the proposed transaction reaches PEAD 200 via path 206 in FIG. 2.

Detailed Description Text (3):
Port 204 may represent an infrared port to facilitate infrared communication with PEAD 200. Alternatively, port 204 may represent a wireless port for facilitating wireless communication. Port 204 may even represent a contact-type connection port, such as a magnetic read/write mechanism or a plug having electrical contacts for directly plugging PEAD 200 into port 204 to facilitate communication. Other techniques to facilitate communication between requesting device 202 and PEAD 200 are readily appreciable to those skilled.

Detailed Description Text (4):
The data pertaining to proposed transaction(s) may then be reviewed by the user, either on a screen 208 of requesting device 202 or optionally on a display screen provided with PEAD 200 (not shown in FIG. 2). If the user approves the transaction, e.g., a purchase of an item for a given amount of money, the user may then signify his approval by activating a switch 210 on PEAD 200, which causes an approval message to be created with the user's identification data, encrypted and transmitted back to requesting device 202 via path 212. If the transaction is not approved, the user may simply do nothing and let the transaction request times out after an elapsed time or may activate another switch on PEAD 200 (not shown in FIG. 1), which causes a reject message, either encrypted or non-encrypted, to be transmitted back to the requesting device 202 via path 212.

Detailed Description Text (5):
The present invention is different from the prior art technique of FIG. 1 in that the user is required in the prior art to enter his identification data into the electronic transaction system, e.g., into ATM 100, to authenticate himself. In contrast, the present invention keeps the identification data related to the user secure within PEAD 200 at all times. Transaction approval occurs within PEAD 200, and the data representing such approval is encrypted, again within PEAD 200, prior to being transmitted to the electronic transaction system, e.g., to requesting

device 202 in FIG. 2.

Detailed Description Text (6):
Accordingly, even if the approval data is intercepted, its encryption would prevent unauthorized users from employing the identification data for illicit purposes. If public key cryptography is employed to encrypt the approval data, the user's private key is also always kept within PEAD 200. Since the user's private key is required for encryption and is unknown to others, even to the electronic transaction system in one embodiment, the encrypted approval data, if intercepted, would be useless to unauthorized third parties even if the approval data can be deciphered using the user's public key. Again, this is different from prior art authentication techniques wherein encryption takes place within the electronic transaction system and requires the entry of the identification data and/or reading the user's private key from the ID card such as an ATM card, a credit card, and the like. As mentioned earlier, the fact that the prior art electronic transaction system requires this identification data and/or user's private key exposes these data to risks, e.g., if the requesting device is not secure or open to data interception via software or hardware.

Detailed Description Text (7):
As another difference, the present invention employs the circuitries within the portable electronic authorization device (PEAD) to perform the approval and encryption of the transaction approval data with in the PEAD itself. In contrast, prior art data cards are essentially passive devices. For example, prior art ATM cards or credit cards only has a magnetic stripe for storing account information and do not have any facility to perform approval and/or encryption of the transaction approval data. While smart cards or IC cards, which are currently being developed, may contain electronic circuitries, current standards for their implementation still requires a reader associated with the requesting device to read out the identification data and/or user's private key in order for the requesting device to perform any approval and/or encryption. A s mentioned earlier, the transmission of these data to the requesting device unnecessarily exposes these data to risks of theft and/or unauthorized interception once transmitted.

Detailed Description Text (9):
As mentioned, transaction approval in the prior art occurs within the electronic transaction system. In contrast, the present invention allows transaction approvals to occur within PEAD 200. The fact that transaction approvals occur entirely within PEAD 200 provides many advantages. By way of example, this feature eliminates the need to have, in one embodiment, the identification data and/or the user's private key in the requesting device. The fact that transaction approvals occur entirely within PEAD 200 (using the user identification data and/or the user's private encryption key that are always kept secure within PEAD 200) substantially enhances the confidentiality of the user identification data and the user's private key, as well as the integrity of the transaction approval process.

Detailed Description Text (10):
Since approval occurs entirely within PEAD 200, the user identification data that is employed to authenticate transactions may be more complicated and elaborate to ensure greater security. By way of example, the user identification data may be more elaborate than a simple password and may include any of the user's name, his birth date, his social security number, or other unique biometrics or unique identifying data such as fingerprint, DNA coding sequence, voice print, or the like. In contrast, prior art authentication techniques limit the user identification data to simple patterns, e.g., simple password of few characters, that are easily memorized by the user since more elaborate identification data may be too difficult to remember or too cumbersome to manually enter. Furthermore, even if the complicated ID data may be stored in the prior art data card, it is still required to be read into the requesting device of the electronic transaction system, again exposing this data to interception or theft once read.

Detailed Description Text (12):
FIG. 3A shows, in one embodiment of the present invention, a simplified schematic of PEAD 200 of FIG. 2, including switch 210. Data path 206 is provided for receiving transaction requests from the electronic transaction system, and data path 212 is provided for transmitting transaction approval data back to the electronic transaction system. It should be borne in mind that although two data paths are discussed herein for ease of understanding, these data paths and other data paths herein may, in one embodiment, represent logical data paths and may be implemented via a single physical data connection. Likewise, the different ports herein may represent, in one embodiment, logical data ports for ease of understanding and may in fact be implemented using a single physical port.

Detailed Description Text (13):
When a transaction request, e.g., a withdrawal transaction from an ATM machine in the amount of $200.00, is transmitted via data path 206 to PEAD 200, this transaction is received by encryption logic 300. At this point, the user may review the proposed transaction, e.g., via the display screen provided with the electronic transaction system and/or PEAD 200, and has a choice to either approve or disapprove the proposed transaction. If the user approves the transaction, he may, in one embodiment, activate a switch 210, which causes the transaction approval data to be created and then encrypted by encryption logic 300 prior to being transmitted back to the electronic transaction system via path 212.

Detailed Description Text (14):
Note that the user identification data block 302, which is employed in the transaction approval process, is not directly coupled to paths 206 and 212. In other words, the memory portion storing the user identification data is intentionally decoupled from the input and output ports of PEAD 200 to prevent direct access thereto.

Detailed Description Text (15):
If access to user identification data 302 is desired, e.g., to approve a transaction, the access can only be made by encryption logic block 300. Likewise, it is not possible to directly access the memory portion 304, which stores the user's private key. If access to user's private key 304 is desired, e.g., to encrypt the transaction approval data, the access can only be made by encryption logic block 300. It should be borne in mind that although user identification 302 and user's private key 304 are shown stored in different memory portions, such illustration is made for ease of understanding and both of these may in fact be stored, in one embodiment, at different addresses on the same memory module.

Detailed Description Text (16):
In some cases, the transaction approval data requires the inclusion of certain pieces of identification data 302. For example, a transaction embodied in the transaction request from the electronic transaction system may be appended with data representative of an "electronic signature" prior to being encrypted and retransmitted back to the electronic transaction system. FIG. 3B shows, in one embodiment, the format of representative transaction approval data 350. With reference to FIG. 3B, transaction data 352, representing a portion of or the entire transaction request received from the electronic transaction system, is appended with certain user identification data 354 and optionally a time stamp 356. The formation of transaction approval data 350 only occurs if the transaction request has already been approved by the user. Once appended, transaction approval data 350 is then encrypted prior to being retransmitted back to the electronic transaction system.

Detailed Description Text (17):
In some cases, it may be desirable to encrypt the transaction request prior to transmission to the PEAD to further enhance security. For example, certain

transaction partners, e.g., vendors or other users on the computer network, may wish to keep the information within a transaction request confidential and may prefer to encrypt the transaction request before furnishing it to the PEAD. Data encryption is also desirable when, for example, the user identification data and the user's private key is written into a blank PEAD for the first time to configure a PEAD that is unique to a given user. The configuration data pertaining the user identification data and the user's private key, while must be written only once into PEAD 200 by the issuer of PEAD 200, is preferably encrypted to render them less vulnerable to theft. Issuers of PEAD 200 may represent, for example, credit card issuers, the government, or any other institution with whom the user maintains an account.

Detailed Description Text (18):
FIG. 4 illustrates, in accordance with one embodiment of the present invention, a schematic of PEAD 200 of FIG. 2. The PEAD 200 of FIG. 4 further employs decryption logic for receiving the encrypted configuration data and optionally the encrypted transaction requests. In FIG. 4, encryption logic 300, user's private key 304, and data paths 206 and 212 are arranged and function substantially as discussed in connection with FIG. 3A.

Detailed Description Text (19):
Transaction requests are normally non-encrypted, i.e., they are received and processed in the manner discussed in connection with FIG. 3A. For highly sensitive transactions, however, the transaction requests may be encrypted and transmitted to PEAD 200 via data path 206 and input into decryption logic 402 to be decrypted. If a public key cryptography is employed, the encrypted transaction requests may be decrypted with a transaction partner public key 404.

Detailed Description Text (20):
Once decrypted, the transaction request is then displayed to the user for approval. The transaction approval data may be furnished to encryption logic 300 via path 406 to be encrypted if approved, e.g., responsive to the activation of switch 210. The encryption is preferably performed with the user's private key 304 if a public key cryptography technique is employed, and the encrypted transaction approval data is then transmitted back to the electronic transaction system via data path 212.

Detailed Description Text (21):
As configuration data typically includes sensitive user identification data and user's private key, it is often encrypted prior to being transmitted to PEAD 200 via data path 408. The encrypted configuration data is received by decryption logic 402 and decrypted therein prior to being written into user identification data block 410 and user's private key block 304. If public key cryptography is employed, the encrypted configuration data may be encrypted by the issuer's private key in the electronic transaction system prior to transmission and decrypted once received by PEAD 200 with an issuer public key 412.

Detailed Description Text (24):
If a greater level of security is desired, the user's private key may be optionally be scrambled or randomized prior to being written into user's private key block 304 by optional scrambler/descrambler logic 413. Scrambler/descrambler logic 413 may, in one embodiment, receive the user's private key, which is furnished by the institution that issues PEAD 200 to the user, and scrambles and/or randomizes it to generate yet another user's private key and a corresponding user's public key. This scrambled/randomized user's private key is then stored in user's private key block 304, which is now unknown even to the issuer of PEAD 200, and the corresponding user's public key may be made known to the issuer and/or the transaction partners to facilitate transactions. Advantageously, there is no other copy of the scrambled/randomized user's private key anywhere else beside within user's private key block 304.

Detailed Description Text (25):
In an alternative embodiment, there may be employed an optional key generation logic 414 which, responsive to a request from the issuing institution, generates the user's private key and the user's public key on its own, i.e., without first requiring the receipt of a user's private key from the issuing institution and randomizing it. The generated user's private key is then stored in private key block 304 and the public key is made known to the issuing institution and/or the transaction partners to facilitate transactions. In this manner, no version of the user's private key, whether randomized or not, exists outside the PEAD itself. As can be appreciated by those skilled in the art, the use of key generation logic 414 further enhances the confidentiality of the user's private key.

Detailed Description Text (28):
A bus 508 couples program/data memory 504 and temporary memory 506 with logic circuitry 502. Communication port 510 represents the communication gateway between PEAD 200 and the electronic transaction system and may be implemented using infrared technology, wireless RF technology, a magnetic read/write head, a contact-type plug for facilitating serial or parallel data transmission, or the like. Communication port may also represent, in one embodiment, a PC card port (popularly known to those skilled as a PCMCIA card). Data path 206 inputs transaction requests into logic circuitry 502 while data path 212 outputs transaction approval data from logic circuitry 502 to the electronic transaction system. Optional data path 408, which has been described in FIG. 4, inputs configuration data into PEAD 200 to write the user identification data and the user's private key into program/data memory 504 to uniquely configure PEAD 200 to a particular user.

Detailed Description Text (31):
Some type of power source, such as a battery, may be provided as well. If PEAD 200 is implemented as a single-chip design, i.e., substantially all components shown in FIG. 5A are fabricated on a single die, then power is external to the die itself. If contact-type communication is employed, e.g., if PEAD 200 must be plugged into the electronic transaction system to conduct transactions, power external to the entire PEAD may be employed for transaction approvals when plugged in, thereby eliminating the size, weight, and cost penalties associated with having a battery onboard the portable transaction apparatus.

Detailed Description Text (32):
In one embodiment, PEAD 200 may be implemented using a general purpose portable computing device, such as any of the miniaturized portable computers or personal digital assistants (PDA's) that are currently popular. A PDA such as the Apple Newton.RTM., for example, may be employed to implement PEAD 200.

Detailed Description Text (33):
FIG. 5B illustrates one implementation of a PEAD wherein the circuitries are implemented on an IC. In FIG. 5B, components having like reference numbers to components in FIG. 5A have similar functions. Data paths 408, 206, and 212, which have been described in connection with FIG. 5A, is coupled to a serial I/O circuit 520, which facilitates data transmission and receipt in a serial manner on data path 522 between PEAD 200 and the electronic transaction system. Vcc pin 524 and ground pin 526, which provide power to PEAD 200 of FIG. 5B, are also shown.

Detailed Description Text (34):
FIG. 5C represents an external view of the PEAD of FIG. 5B after being embedded in a card-like package for ease of carrying and insertion into a serial I/O port of the electronic transaction system. Card 550, which embeds the integrated circuit implementing the inventive PEAD, includes, in one embodiment, four external contacts. External serial contacts 552 and 554 carry data and ground respectively to facilitate serial communication with a serial device of an electronic transaction system. External Vcc contact 524 and external ground contact 526, which supply power to the PEAD as discussed in connection with FIG. 5A, are also shown.

When card 550 is inserted into an electronic transaction system, it is powered through external contacts 524 and 526, thereby enabling the PEAD circuitries therein to receive transaction requests via external serial contacts 552 and 554, approve the requests within the PEAD if appropriate, encrypt transaction approval data within the PEAD circuitries, and serially communicate the encrypted transaction approval data to the electronic transaction system via external serial contacts 552 and 554.

Detailed Description Text (35):
FIG. 6A represents an external view of a PEAD in accordance with a preferred embodiment of the present invention. PEAD 200 of FIG. 6A is preferably implemented as a small, self-containing package that is sufficiently ruggedized for daily use in the field. Preferably, PEAD 200 of FIG. 6A is small enough to be comfortably carried with the user at all times, e.g., as a key chain attachment or a small package that can easily fit inside a purse or a wallet. The physical enclosure of PEAD 200 is preferably arranged such that the content will be tamper-proof (i.e., if it is opened in an unauthorized manner then the user's private key and/or the user identification data will be destroyed or the PEAD will no longer be able to approve transactions). By way of example, the enclosure may be arranged such that if it is opened, there is a change in the flow of current in a current path, e.g., either the existing current flow is interrupted or a current path that has been idle starts to flow. The change in the flow of current may then force RESET.

Detailed Description Text (36):
There is shown an infrared communication port 602 for receiving and transmitting data vis-a-vis the electronic transaction system. A small on/off switch 604 permits the user to turn off the PEAD to conserve power when not in use. Approve button 606 permits the user to signify approval of a proposed transaction. Optional skip button 608 permits the user to indicate rejection of a particular transaction. Skip button 608 may be omitted since a transaction request may be understood, in some embodiment, as not being approved if approve button 606 is not activated within a given period of time after receiving the request.

Detailed Description Text (37):
Optional display 610 may be implemented using any type of display technology such as liquid crystal technology. Displays 610 displays, among others, the transaction being proposed for approval. Display 610 may be omitted if desired, in which case the transaction may be viewed, for example, at a display associated with the electronic transaction system itself. Optional user authentication mechanism 612 prevents PEAD 200 from being used for approving transactions unless the user is able to identify himself to PEAD 200 as the rightful and authorized user. Optional user authentication mechanism 612 may require the user to enter a password, to furnish a fingerprint or a voice print, or other biometrics and/or identifying characteristics specific to the authorized user before PEAD 200 can be activated and employed for approving transactions.

Detailed Description Text (38):
FIG. 6B illustrates, in a simplified manner and in accordance with one aspect of the present invention, the hardware for implementing PEAD 200 of FIG. 6A. Battery 652 provides power to the circuitry of PEAD 200. A microcontroller 654 executes codes stored in flash memory 656 and employs random access memory 658 for the execution. In one embodiment, microcontroller 654, flash memory 656, and even random access memory 658 may be implemented on a single chip, e.g., a NC68HC05SCXX family chip from Motorola Inc. of Schaumburg, Ill. such as the NC68HC05SC28. Approve button 606 and optional skip button 608 are coupled to microcontroller 654 to permit the user to indicate approval or rejection of a particular transaction displayed using display circuitry 660. Communication to and from the electronic transaction system is accomplished under control of microcontroller 654 via an infrared transceiver 662. Power switch 664 permits the user to power off PEAD 200 when not in use to conserve power and to prevent accidental approval.

Detailed Description Text (39):
FIG. 7 is a flowchart illustrating, in accordance with one aspect of the present invention, the approval technique employing the inventive PEAD. In step 702, a transaction request is received at the PEAD from the requesting device associated with the electronic transaction system. In step 704, the user has the option whether to approve or disapprove the transaction proposed. If not approved, e.g., either by activating the skip button of the PEAD or simply allowing the request to time out, nothing will be done.

Detailed Description Text (40):
On the other hand, if the user approves the proposed transaction, the user may activate the approve button to create transaction approval data. The transaction approval data is then encrypted in step 708 within the PEAD. In step 710, the encrypted transaction approval data is transmitted to the requesting device of the electronic transaction system after being encrypted.

Detailed Description Text (41):
FIG. 8 is a flowchart illustrating, in accordance with one aspect of the present invention, the steps involved in encrypting transaction approval data using public key cryptography. In step 802, the transaction approval data package is created. As discussed earlier in connection with FIG. 3B, the transaction approval data may be created by appending any necessary user identification data to a portion of or the entire transaction request. Optionally, a time stamp may also be appended thereto. In step 804, the transaction approval data is encrypted using the user's private key, which is preferably kept secured at all times within the PEAD. Thereafter, the encrypted transaction approval data is transmitted back to the electronic transaction system.

Detailed Description Text (42):
In accordance with one aspect of the present invention, it is recognized that even if the encrypted transaction approval data is intercepted and decrypted for analysis by a third party, it is not possible to bypass the security features of the invention as long as the user's private key or the user identification data is secure. As mentioned earlier, since the user identification data is not accessible externally, it is always secure within the PEAD. This is unlike the prior art wherein the user is required to enter the identification data, e.g., password, at the electronic transaction system and risks exposure of this sensitive data.

Detailed Description Text (43):
Even if the user identification data is compromised, transaction approval still cannot take place unless there is possession of the user's private key. It would be useless to intercept the encrypted transaction approval data even if one can decrypt it using the user's public key since the transaction partner, e.g., the merchant requesting approval of the transaction, will not accept any transaction approval data not encrypted using the user's private key. Again, since the private key is not accessible externally, it is always secure within the PEAD. This aspect of the invention has great advantages in performing on-line transactions since the user's private key no longer has to be stored in a vulnerable computer file in a workstation, which may be accessible by other parties and may be difficult to conveniently tote along for other authentication tasks.

Detailed Description Text (44):
The fact that the PEAD is implemented in a small, portable package makes it convenient and comfortable for the user to maintain the PEAD within his possession at all times. Even if the PEAD is physically stolen, however, the optional user authentication mechanism, e.g., user authentication mechanism 612 of FIG. 6A, provides an additional level of protection and renders the PEAD useless to all but the properly authenticated user. Of course the user can always notify the issuer of the PEAD if the PEAD is stolen or lost, and the issuer can inform transaction

partners to refuse any transaction approval data encrypted with the user's private key of the stolen PEAD.

Detailed Description Text (45):
The fact that the transaction approval data includes the time stamp, the merchant's name, the amount approved, and other relevant data also enhances the integrity of the transaction approval process. If the merchant inadvertently or intentionally submits multiple transaction approvals to the issuer, the issuer may be able to recognize from these data items that the submissions are duplicates and ignore any duplicate transaction approval data. For example, the issuer may recognize that is it unlikely for a user to purchase multiple identical dinners at the same restaurant at a given time and date.

Detailed Description Text (46):
While this invention has been described in terms of several preferred embodiments, there are alterations, permutations, and equivalents which fall within the scope of this invention. It should also be noted that there are many alternative ways of implementing the methods and apparatuses of the present invention. By way of example, while the discussion herein has focused on transaction approvals, it should be apparent to those skilled that the PEAD may be employed to conduct any kind of transaction vis-a-vis an electronic transaction system any time secured data transmission from the user to the electronic transaction system is preferred. For example, the PEAD may be employed for logging into highly sensitive computer systems or facilities. When so implemented, the computer terminal with which the PEAD communicates may be equipped with an infrared port, a magnetic reader port, or a contact-type plug for communication with the PEAD. The user may then employ the PEAD to perform any type of authentication tasks online.

Detailed Description Text (47):
As a further example, the PEAD may be employed to "sign" any computer file for authentication purposes (e.g., to authenticate the date or the user). The transaction approval data may then be saved along with the file to be authenticated for future reference. Note that the transaction authentication data is again tamper-proof since any transaction authentication data not encrypted using the user's private key will not be accepted as authentic. Also, it should be apparent that if the PEAD is employed to approve only predefined transactions, the transaction data may be stored in advance within the PEAD and do not need to be received from externally by the PEAD. It is therefore intended that the following appended claims be interpreted as including all such alterations, permutations, and equivalents as fall within the true spirit and scope of the present invention.

Current US Class (1):
235

CLAIMS:

1. In a portable electronic authorization device, a method for approving a transaction request originated from an electronic transaction system, comprising:

receiving at said portable electronic authorization device first digital data, said first digital data representing said transaction request; and

if said transaction request is approved by a user of said portable electronic authorization device, transmitting a second digital data to said electronic transaction system, said second digital data being encrypted by circuitries within said portable electronic authorization device and signifies said user's approval of said transaction request.

2. The method of claim 1 wherein said second digital data includes at least a portion of said transaction request.

3. The method of claim 1 wherein said second digital data is encrypted with a user's private key using public key cryptography, said user's private key being kept within said portable electronic authorization device thereby eliminating a need to exchange said user's private key between said portable electronic authorization device and said electronic transaction system for approving said transaction request.

5. The method of claim 1 further comprising:

authenticating said user prior to permitting said user to approve said transaction request using said portable electronic authorization device, said authenticating requires one of a password, a finger print, a voice print at a user authentication mechanism associated with said portable electronic authorization device.

6. The method of claim 1 wherein said transmitting said second digital data is performed via an infrared communication port associated with said portable electronic authorization device.

7. The method of claim 1 wherein said transmitting said second digital data is performed via a contact-type serial communication port associated with said portable electronic authorization device.

8. The method of claim 1 further comprising displaying said transaction request for viewing by said user on a display screen associated with said portable electronic authorization device.

9. The method of claim 1 wherein said transaction request represents a request for authenticating an electronic file, said second digital data includes an electronic signature for authenticating said electronic file.

10. The method of claim 1 further comprising activating an approval switch associated with said portable electronic authorization device if said transaction request is approved by said user, said activating said approval switch causing said second digital device to be transmitted from said portable electronic authorization device to said electronic transaction system.

11. The method of claim 1 wherein said first digital data represents an encrypted version of said transaction request encrypted using public key cryptography with a private key associated with a transaction partner, wherein said receiving further comprising decrypting, using decryption logic associated with said portable electronic authorization device, said first digital data using a public key associated with said transaction partner.

14. The method of claim 1 wherein said transmitting said second digital data is performed via a PC card communication port associated with said portable electronic authorization device.

15. The method of claim 14 wherein said transaction request represents a transaction request for a transaction conducted via a computer network, said electronic transaction system includes a computer coupled to said computer network, said portable electronic authorization device configured for plugging into a PC card slot of said computer to facilitate said receiving said first digital data.

17. The method of claim 1 wherein said second digital data comprises at least a portion of said transaction request, said transaction approval data further comprising identification data pertaining said user and a time stamp.

18. The method of claim 1 further comprising configuring said portable electronic authorization device for said user by receiving configuration data from an issuer

of an account capable of transaction via said portable electronic authorization device, said configuration data includes at least one of identification data pertaining said user and said private key.

19. The method of claim 1 wherein said transmitting said second digital data is performed via a wireless RF communication port associated with said portable electronic authorization device.

20. The method of claim 1 wherein said transmitting said second digital data is performed via a contact-type parallel communication port associated with said portable electronic authorization device.

21. A portable electronic authorization device for approving a transaction request originated from an electronic transaction system, comprising:

means for receiving at said portable electronic authorization device first digital data, said first digital data representing said transaction request;

means within said portable electronic authorization device for forming second digital data responsive to a receipt of said transaction request if a user of said portable electronic authorization device approves said transaction request, said second digital data representing encrypted data signing said user's approval of said transaction request; and

means, coupled to said forming means, for transmitting said second digital data to said electronic transaction system.

22. The portable electronic authorization device of claim 21 wherein said second digital data includes at least a portion of said transaction request.

23. The portable electronic authorization device of claim 21 further including first memory means coupled to said forming means for storing a user's private key for use in forming said second digital data in accordance with a public key cryptography technique, wherein said forming means includes encrypting means coupled to said first memory means for creating said encrypted data with said user's private key using said public key cryptography technique, whereby said presence of said user's private key in said first memory means eliminates a need to exchange said user's private key between said portable electronic authorization device and said electronic transaction system for approving said transaction request.

25. The portable electronic authorization device of claim 23 further comprising means, coupled to said first memory means, for configuring said portable electronic authorization device for said user, said configuring means receives configuration data from an issuer of an account capable of transaction via said portable electronic authorization device, said configuration data includes at least one of identification data pertaining said user and said private key; and

means for writing said configuration data to memory of said portable electronic authorization device.

26. The portable electronic authorization device of claim 21 further comprising:

means coupled to said forming means for authenticating said user prior to permitting said user to approve said transaction request using said portable electronic authorization device, said authenticating means requires one of a password, a finger print, and a voice print.

27. The portable electronic authorization device of claim 21 wherein said means for transmitting said second digital data includes means for communicating with said

electronic transaction system using infrared signals.

28. The portable electronic authorization device of claim 21 wherein said means for transmitting said second digital data includes means for communicating with said electronic transaction system using wireless RF signals.

29. The portable electronic authorization device of claim 21 wherein said means for transmitting said second digital data includes a contact-type serial port for communicating with said electronic transaction system.

30. The portable electronic authorization device of claim 21 wherein said means for transmitting said second digital data includes a contact-type parallel port for communicating with said electronic transaction system.

31. The portable electronic authorization device of claim 21 further comprising means, coupled to said receiving means, for displaying said transaction request for viewing by said user.

32. The portable electronic authorization device of claim 21 further comprising means, coupled to said forming means, for said user to indicate that said transaction request is approved, said means for said user to indicate that said transaction request is approved causes said second digital data to be transmitted from said portable electronic authorization device to said electronic transaction system.

33. The portable electronic authorization device of claim 32 wherein said means for said user to indicate that said transaction request is approved represents a switch configured for activation by said user.

34. The portable electronic authorization device of claim 21 wherein said first digital data represents an encrypted version of said transaction request, said first digital data being encrypted using public key cryptography with a private key associated with a transaction partner, wherein said means for receiving further comprising means for decrypting said first digital data using a public key associated with said transaction partner.

37. The portable electronic authorization device of claim 21 wherein said means for transmitting said second digital data includes a first PC card communication port associated with said portable electronic authorization device.

38. The portable electronic authorization device of claim 37 wherein said transaction request represents a transaction request for a transaction conducted via a computer network, said electronic transaction system includes a computer coupled to said computer network, said portable electronic authorization device being configured for plugging into a second PC card communication port of said computer to facilitate receiving said first digital data.

40. The portable electronic authorization device of claim 21 wherein said second digital data comprises at least a portion of said transaction request, said second digital data further comprising identification data pertaining said user and a time stamp.

41. The portable electronic authorization device of claim 21 wherein said transaction request represents a request for authenticating an electronic file, said second digital data includes an electronic signature for authenticating said electronic file.

42. A portable electronic authorization device for approving a transaction request originated from an electronic transaction system, comprising:

first logic circuit configured to receive first digital data representative of said transaction request;

second logic circuit configured to form second digital data responsive to said transaction request received by said first logic circuit if said transaction request is approved by a user of said portable electronic transaction device, said second digital data representing encrypted data signifying an approval by said user of said transaction request; and

transmission circuitry coupled to said second logic circuit, said transmission circuitry being configured to transmit said second digital data from said portable electronic authorization apparatus to said electronic transaction system if said user approves said transaction request.

43. The portable electronic authorization device of claim 42 wherein said second digital data includes at least a portion of said transaction request.

44. The portable electronic authorization device of claim 42 wherein said first digital data represents an encrypted version of said transaction request, said first digital data being encrypted using public key cryptography with a private key associated with a transaction partner, wherein said first logic circuit comprises decrypting circuitry configured to decrypt said first digital data using a public key associated with said transaction partner.

45. The portable electronic authorization device of claim 44 further including first memory circuit coupled to said decrypting circuitry, said first memory circuit being configured for storing a user's private key for use in forming said second digital data in accordance with a public key cryptography technique, wherein said second logic circuit includes encrypting logic coupled to said first memory circuit for creating said encrypted data with said user's private key using said public key cryptography technique, whereby said presence of said user's private key in said first memory circuit eliminates a need to exchange said user's private key between said portable electronic authorization device and said electronic transaction system for approving said transaction request.

47. The portable electronic authorization device of claim 46 wherein said first logic circuit comprises receiving circuit coupled to said decrypting logic, said receiving circuit being configured to receive said first digital data from said electronic transaction system prior to passing said first digital data to said decrypting logic for decryption, said receiving circuit being decoupled from said first memory circuit, wherein said user's private key stored in said first memory circuit is inaccessible directly by said receiving logic, thereby preventing said user's private key from being accessed from externally without traversing said decrypting logic.

49. The portable electronic authorization device of claim 42 further comprising:

user authentication mechanism coupled to said second logic circuit, said user authentication mechanism being configured to authenticate said user prior to permitting said user to approve said transaction request using said portable electronic authorization device, said authentication mechanism requires one of a password, a finger print, and a voice print.

50. The portable electronic authorization device of claim 42 wherein said transmission circuitry includes circuitry configured for communicating with said electronic transaction system using infrared signals.

51. The portable electronic authorization device of claim 42 wherein said transmission circuitry includes circuitry configured for communicating with said electronic transaction system using wireless RF signals.

52. The portable electronic authorization device of claim 42 wherein said transmission circuitry includes a contact-type serial port for communicating with said electronic transaction system.

53. The portable electronic authorization device of claim 42 wherein said transmission circuitry includes a contact-type parallel port for communicating with said electronic transaction system.

54. The portable electronic authorization device of claim 42 further comprising a display coupled to said first logic circuit, said display being configured to display said transaction request for viewing by said user.

55. The portable electronic authorization device of claim 42 further comprising a switch coupled to said second logic circuit, said switch permitting said user to indicate through activating said switch that said transaction request is approved by said user.

58. The portable electronic authorization device of claim 42 wherein said transmission circuitry includes a PC card communication port associated with said portable electronic authorization device.

59. The portable electronic authorization device of claim 58 wherein said transaction request represents a transaction request for a transaction conducted via a computer network, said electronic transaction system includes a computer coupled to said computer network, said portable electronic authorization device being configured for plugging into a PC card slot of said computer to facilitate receiving said first digital data.

61. The portable electronic authorization device of claim 42 wherein said second digital data comprises at least a portion of said transaction request, said second digital data further comprising identification data pertaining said user and a time stamp.

62. The portable electronic authorization device of claim 42 wherein said transaction request represents a request for authenticating an electronic file, said second digital data includes an electronic signature for authenticating said electronic file.

63. In a portable electronic authorization device, a method for approving a transaction request originated from an electronic transaction system, comprising:

receiving at said portable electronic authorization device first digital data, said first digital data representing said transaction request;

if said transaction request is approved by a user of said portable electronic authorization device, generating second digital data, said second digital data representing transaction approval data signifying said user's approval of said transaction request;

encrypting within said portable electronic authorization device said second digital data, thereby creating third digital data representing an encrypted version of said second digital data; and

transmitting said third digital data from said portable electronic authorization device to said electronic transaction system, thereby permitting said electronic transaction system to ascertain whether said transaction request is approved by said user.

64. The method of claim 63 wherein said encrypting is performed using a public key

cryptography technique, said portable electronic authorization device containing a user's private key for encrypting said second digital data to form said third digital data, thereby eliminating a need to transmit said user's private key from said portable electronic authorization device to said electronic transaction system, said third digital data being configured for being decrypted at said electronic transaction system using a user's public key.

66. The method of claim 63 further comprising:

authenticating said user prior to permitting said user to approve said transaction request using said portable electronic authorization device, said authenticating requires one of a password, a finger print, a voice print at a user authentication mechanism associated with said portable electronic authorization device.

67. The method of claim 63 wherein said user's private key is generated using a key generation logic within said portable electronic authorization device, thereby eliminating a need to transmit said user's private key from said electronic transaction system to said portable electronic authorization device.

68. The method of claim 63 wherein said transmitting said third digital data is performed via an infrared communication port associated with said portable electronic authorization device.

69. The method of claim 63 wherein said transmitting said third digital data is performed via a wireless RF communication port associated with said portable electronic authorization device.

70. The method of claim 63 wherein said transmitting said third digital data is performed via a contact-type parallel communication port associated with said portable electronic authorization device.

71. The method of claim 63 wherein said transmitting said third digital data is performed via a contact-type serial communication port associated with said portable electronic authorization device.

72. The method of claim 63 further comprising displaying said transaction request for viewing by said user on a display screen associated with said portable electronic authorization device.

73. The method of claim 63 further comprising activating an approval switch associated with said portable electronic authorization device if said transaction request is approved by said user.

74. The method of claim 63 wherein said first digital data represents an encrypted version of said transaction request encrypted using public key cryptography, wherein said receiving further comprising decrypting, using decryption logic associated with said portable electronic authorization device, said first digital data using a transaction partner's public key.

77. The method of claim 63 wherein said transmitting said third digital data is performed via a PC card communication port associated with said portable electronic authorization device.

78. The method of claim 77 wherein said transaction request represents a transaction request for a transaction conducted via a computer network, said electronic transaction system includes a computer coupled to said computer network, said portable electronic authorization device configured for plugging into a PC card slot of said computer to facilitate said receiving said first digital data.

80. The method of claim 63 wherein said transaction approval data comprises at

least a portion of said transaction request, said transaction approval data further comprising identification data pertaining said user and a time stamp.

81. The method of claim 63 further comprising configuring said portable electronic authorization device for said user by receiving configuration data from an issuer of an account capable of transaction via said portable electronic authorization device, said configuration data includes at least one of identification data pertaining said user and said private key.

82. The method of claim 63 wherein said transaction request represents a request for authenticating an electronic file, said transaction approval data includes an electronic signature attached to said electronic file.

Previous Doc Next Doc Go to Doc#